

2007-CDOS-SEQ-001-0403

**SEQUOIA VOTING
SYSTEMS**

**PROJECT
OVERVIEW
“A.4”**

ORIGINAL

**2007-CDOS-SEQ-001-0403
PROJECT OVERVIEW BINDER “A.4”**

TABLE OF CONTENTS

**2007-CDOS-SEQ-001-0403
PROJECT OVERVIEW BINDER “A.4”**

TABLE OF CONTENTS

- 1. INTRODUCTION**
 - a. Introduction Statement**
 - b. Detailed Test Summary**
- 2. COMPONENTS**
 - a. Components of the Sequoia voting system package**
- 3. RECOMMENDATION**
 - a. Recommendation Overview**
 - b. Voting system application recommendation**
 - c. Bar charts of residual failures**
- 4. RESTRICTIONS**
 - a. Restrictions for use of the voting system**
- 5. CONDITIONS**
 - a. Conditions for use of the voting system**
- 6. COMMENTS**
 - a. Comments from testing board members**
- 7. AUDIT REPORTS**
 - a. Testing Board response to audit report**
 - b. Audit Report**
 - c. Associated correspondence – Located in Binder “A”, Sec. 7**
- 8. ADDITIONAL CORRESPONDENCE – Located in Binders “B - C”**

**2007-CDOS-SEQ-001-0403
PROJECT OVERVIEW BINDER “A.4”**

INTRODUCTION

STATE OF COLORADO
Department of State

1700 Broadway, Suite 270
Denver, CO 80290



Mike Coffman
Secretary of State

Holly Lowder
Director, Elections

Introduction

Why an Amendment to the A.3 binder/report?

Acting in accordance with HB08-1155, the Secretary of State requested the Testing Board to evaluate conditions after listening to testimony from county officials and the voting system vendor. Additionally, HB08-1155 allowed the Testing Board to consider county security procedures in the evaluation of conditions for the voting system. The meetings, discussion and draft versions of conditions were open to the public.

The sections of this binder have been modified to support the outcome of the additional testing.

Why an amendment to the A.2 binder/report?

During the review of the findings with the vendor after the certification announcement the vendor made claims that certain security items could be mitigated if the Testing Board was aware of certain options within the system. One particular matter that struck a chord with the Testing Board is the fact that the Edge II device does indeed have an option for a printer test between V-VPAT paper changes.

Although a seemingly small matter, this sole piece of information is necessary for a workaround to ensure that all electronic records have corresponding V-VPAT records for increased audits. The vendor provided the documentation on the process and the system was tested and documented by the Testing Board to perform this specific function. Notes have been added to the conditions section to require the use of the procedure to mitigate deficiencies and allow increased confidence in a good audit of the paper records of the device.

The remainder of the sections of the binder have been updated to reflect these changes which include the recommendation section, the restriction section and the conditions section.

Introduction

On April 3, 2007, Sequoia Voting Systems approached the Colorado Secretary of State's Office with an application to certify a voting system. The application was accepted by the Voting Systems Certification Program Testing Board (Testing Board). The system was assigned certification number: 2007-CDOS-SEQ-001-0403.

The voting system is known by its federal certification name as "WinEDS 3.1.074." Federal certification is to the 2002 VSS standards, and was obtained on October 23rd, 2006 (NASED#: N-1-07-22-22-004).

The Testing Board proceeded to evaluate the Sequoia voting system during the time period of April 3rd – December 1st. All findings are documented within the binders A.3 – 31, as well as addendum binders: 7.1, 13.1, 14.1, 16.1, 17.1, 18.1, 19.1, 21.1, 22.1, 23.1, 24.1, 25.1, 25.2, and 26.1.

The Project Overview Binders (Binders "A – C including addendum binders") provides an overview of the findings of the project, and the following additional information:

- Introduction
- System Components
- Recommendation to the Secretary of State
- Restrictions on the use of the voting system suggested by the Testing Board
- Conditions to the Recommendation suggested by the Testing Board
- Additional Comments by the Testing Board
- Independent Audit Reports
- Miscellaneous Correspondence of importance

During the process of certifying the system, the Testing Board adhered to the procedures outlined by the Voting System Program procedures document. The certification process was led by Jerome Lovato, with Tim Bishop and Michael Chadwell providing the primary cross evaluation. Additional cross check and documentation verification was conducted by Danny Casias with additional coordination by the Program Manager – John Gardner with assistance from Tim Bishop as necessary.

The Testing Board evaluated the voting system in accordance with the requirements set forth in Secretary of State Rule 45, as well as applicable elements contained within the laws of the Help America Vote Act, Colorado Revised Statute, multiple sections of Title 1, and Secretary of State Rules as appropriate. All testing results and output which includes extensive video documentation of the evaluation process have been archived and well preserved in accordance with the Voting Systems Program procedures document.

Through the evaluation, the Testing Board identified a variety of deficiencies within the system which include functionality, security, auditability and documentation requirements. The following sections will address these deficiencies as either a restriction for use (preventing recommendation by the Testing Board), or a condition for use (allowing the system to be recommended provided conditional elements are adhered to). Restrictions are identified in a one-to-one value. One identified restriction = one failure on the Detail Test Summary. Conditional elements represent a one-to-many value. The execution of a single condition placed on the use of the system in many cases will address multiple failures as the Testing Board often experienced failures that exhibited a "daisy chain" effect. One high level failure would trigger many follow up test scenarios. Refer to the comments section of this binder for additional comments on this topic.



Detailed Test Summary

The Testing Board executed the testing process for the Sequoia Voting System in the manner prescribed by Rule 45, and the detailed procedures document provided on the Voting Systems State Certification Program website (<http://www.elections.colorado.gov/DDefault.aspx?tid=501>).

The outcome of the process involved over 700 functional test evaluations, 4405 detailed line items for document review, and over 90 supplemental tests comprising the sections for application review, demonstration and work on completing the trusted build. The documentation comprised of this test work is evident in over 50 binders generated by the Testing Board, a multitude of boxes containing evidence generated from devices, ballots, reports, and other findings. In addition to this evidence, over 200 DVD records exist documenting the process of the Testing Board.

Below is the summary report of test status generated by the Testing Board regarding the Sequoia Voting System evaluation:

Sequoia						
	# Requirements	# Passed	# Failed	Binder Status		% Passed
Phase I - Application	22	14	8	signed		63.64%
Phase II - Doc. Review	4406	3259	1136	signed		73.97%
Phase III - Demo	54	49	5	signed		90.74%
Phase III - Trusted Build	20	12	6	signed		60.00%
Phase III - Functional Test (overall)	737	566	171		100.00%	76.80%
Security	139	113	26			81.29%
System Process	339	255	84			75.22%
Election (pre, ED and post)	259	198	61			76.45%
Independent Audit	1674	1674		Review of Test Board work.		100.00%
Phase IV - Certification Doc.	n/a	n/a	n/a	n/a	n/a	
Phase V - Qualification Report	n/a	n/a	n/a	n/a	n/a	

Requirements Status for Colorado Certification of Sequoia Voting System

Section Category	Binder #	Category	Seq	Total # of Tests to complete	Status:	DRE (edge 2)	DRE Edge 2 plus)	PCOS	CCOS	EMS	Remaining to complete
Section "A" - Pre Testing	1	Application	aa	22	Pass	n/a	n/a	n/a	n/a	13	0
					Pass Conditional	n/a	n/a	n/a	n/a	1	
					Suspend	n/a	n/a	n/a	n/a		
					Fail	n/a	n/a	n/a	n/a	8	
					Not applicable	n/a	n/a	n/a	n/a		
	2-6	Documentation Review	ab	4405	Pass	381	48	289	273	276	0
					Pass Conditional						
					Suspend						
					Fail	92	452	134	89	84	
					Not applicable	408	381	458	519	521	
	7	Demonstration	ac	54	Pass	5	5	10	10	12	0
					Pass Conditional	1	1	2	2	1	
					Suspend						
					Fail	1	1	1	1	1	
					Not applicable						
	8	Trusted Build	ad	20	Pass	2		4	2	2	0
					Pass Conditional						
					Suspend						
					Fail	2			2	2	
					Not applicable	1		1	1	1	
9-12	Source Code Review	ae	0	Not applicable	n/a	n/a	n/a	n/a	n/a	0	

Requirements Status for Colorado Certification of Sequoia Voting System

Section Category	Binder #	Category	Seq	Total # of Tests to complete	Status:	DRE (edge 2)	DRE Edge 2 plus)	PCOS	CCOS	EMS	Remaining to complete	
Section "B" - Security Testing	13	System Access	ba	36	Pass	1		1		9	0	
					Pass Conditional							
					Suspend							
					Fail	5		4	5	6		
					Not applicable	1		2	1	1		
	14	Operating System Security	bb	20	Pass						0	
					Pass Conditional							
					Suspend							
					Fail					2		
					Not applicable	4	5			9		
	15	Database Security	bc	24	Not applicable	3	3	6	6	6	0	
	16	Removable Media	bd	13	Pass					1	1	0
					Pass Conditional							
					Suspend							
					Fail	1		1		1		
					Not applicable	1	1	2	2	2		
	17	Networking and Telecommunications	be	46	Pass	3		2	4	4	0	
					Pass Conditional	1		1		1		
					Suspend							
					Fail	1						
Not applicable					7		9	7	6			

Requirements Status for Colorado Certification of Sequoia Voting System

Section Category	Binder #	Category	Seq	Total # of Tests to complete	Status:	DRE (edge 2)	DRE Edge 2 plus)	PCOS	CCOS	EMS	Remaining to complete
Section "C" - System Testing	18	System	ca	47	Pass	6		3		12	0
					Pass Conditional						
					Suspend						
					Fail	3		5		16	
					Not applicable					2	
	18	System (central count)	cb	11	Pass	n/a	n/a	n/a	3	n/a	0
					Pass Conditional	n/a	n/a	n/a		n/a	
					Suspend	n/a	n/a	n/a		n/a	
					Fail	n/a	n/a	n/a	4	n/a	
					Not applicable	n/a	n/a	n/a	4	n/a	
	19-20	Ballot Process	cc	152	Pass	21		38	27	25	0
					Pass Conditional	1					
					Suspend						
					Fail	2		6	5	1	
					Not applicable	1		2	14	9	
	21	Performance	cd	24	Pass	1		2	1	4	0
					Pass Conditional						
					Suspend						
					Fail	7		3	4	2	
					Not applicable						
	21	DRE Processing	ce	24	Pass	12		n/a	n/a	n/a	0
					Pass Conditional	2		n/a	n/a	n/a	
					Suspend			n/a	n/a	n/a	
					Fail	3		n/a	n/a	n/a	
					Not applicable	7		n/a	n/a	n/a	
	22	Audits	cf	29	Pass	6		5	4	1	0
					Pass Conditional						
					Suspend						
Fail					1		2	3	7		
Not applicable											
22	Reports	cg	52	Pass	6		7	4	9	0	
				Pass Conditional							
				Suspend							
				Fail	2		3	4	1		
				Not applicable	5		5	3	3		

Requirements Status for Colorado Certification of Sequoia Voting System

Section Category	Binder #	Category	Seq	Total # of Tests to complete	Status:	DRE (edge 2)	DRE Edge 2 plus)	PCOS	CCOS	EMS	Remaining to complete	
Section "D" - Election Day Tests	23	Hardware Diagnostics Testing	da	8	Pass	1		1				0
					Pass Conditional							
					Suspend							
					Fail	1			1			
					Not applicable			1	1	2		
	23	Voting	db	65	Pass	14		19	19	6		0
					Pass Conditional							
					Suspend							
					Fail	1			1			
					Not applicable	2		1	1	1		
	24	Multi-Page Ballots	dc	6	Pass			2	1	1		0
					Pass Conditional							
					Suspend							
					Fail							
					Not applicable	2						
	24	Multiple Languages	dd	4	Pass	1		1	1	1		0
					Pass Conditional							
					Suspend							
					Fail							
					Not applicable							
	24	Provisional	de	25	Pass	3		1	3	3		0
					Pass Conditional	1						
					Suspend							
					Fail	3		2	2	2		
					Not applicable			3	1	1		
	25	V-VPAT	df	28	Pass	23		n/a	n/a	n/a		0
					Pass Conditional	1		n/a	n/a	n/a		
					Suspend			n/a	n/a	n/a		
Fail					2	1	n/a	n/a	n/a			
Not applicable					1		n/a	n/a	n/a			
25	Accessibility	dg	80	Pass	29	17	n/a	n/a	n/a		0	
				Pass Conditional	1		n/a	n/a	n/a			
				Suspend			n/a	n/a	n/a			
				Fail	9	22	n/a	n/a	n/a			
				Not applicable	2		n/a	n/a	n/a			
26	Closing Polls	dh	30	Pass	10		10	n/a	n/a		0	
				Pass Conditional				n/a	n/a			
				Suspend				n/a	n/a			
				Fail	5		5	n/a	n/a			
				Not applicable				n/a	n/a			

Requirements Status for Colorado Certification of Sequoia Voting System

Section Category	Binder #	Category	Seq	Total # of Tests to complete	Status:	DRE (edge 2)	DRE Edge 2 plus)	PCOS	CCOS	EMS	Remaining to complete
Section "E" - Post Election	27	Post Election Audit	ea	4	Pass					1	0
					Pass Conditional						
					Suspend						
					Fail	1		1	1		
					Not applicable						
	27	Recount	eb	8	Pass			2	2	1	0
					Pass Conditional	1					
					Suspend						
					Fail				1		
					Not applicable	1					
	27	Recount (central count)	ec	1	Pass	n/a	n/a	n/a	1	n/a	0
					Pass Conditional	n/a	n/a	n/a		n/a	
					Suspend	n/a	n/a	n/a		n/a	
					Fail	n/a	n/a	n/a		n/a	
					Not applicable	n/a	n/a	n/a		n/a	

Archive Storage Boxes for the Sequoia Voting System Certification Process:



Backup Binders documenting the Sequoia Voting System Certification Process (original binders moved to archive storage upon completion of process):



**2007-CDOS-SEQ-001-0403
PROJECT OVERVIEW BINDER “A.4”**

COMPONENTS

STATE OF COLORADO
Department of State

1700 Broadway, Suite 270
Denver, CO 80290



Mike Coffman
Secretary of State

Holly Lowder
Director, Elections

Components

As submitted on April 3, 2007, the following components comprise the requested voting system package from Sequoia Voting Systems:

Component Name	System Function	Version Number
WinEDS	Software Application	3.1.074
Optech Insight / Insight Plus	Precinct Optical Scanner which includes: Insight Memory Pack Receiver	HPX K1.44/APX 2.12 2.15
Optech 400-C	Central Count Optical Scanner which includes: WinETP software	3.00 1.14.3
AVC Edge II	Direct Record Electronic Device which includes: Card Activator or HAAT Model 50 VeriVote Edge Audio Unit	5.0.31 5.0.31 2.1.18 4.3 5.0 Rev. C
AVC Edge II Plus	Direct Record Electronic Device which includes: HAAT Model 50 or Card Activator	1.2.33 2.1.18 5.0.31

Photographs and additional details on each component can be found under test # AA6-P1-605.

**2007-CDOS-SEQ-001-0403
PROJECT OVERVIEW BINDER “A.4”**

RECOMMENDATION



Recommendation Overview

The approach of the Testing Board regarding a recommendation is absolute. Any one item outstanding in the **Restrictions** section of the binder (no “conditional use” option discoverable by the Testing Board) will trigger a “N” value on the **Recommendation** table.

Therefore, for quick understanding of the overall outstanding deficiencies with the system, and to provide a summary of reasons for the “Y” or “N” value in the **Recommendation** table.

The following table provides a high level summary statement of findings by the Testing Board. These items constitute a summary of the findings in the **Restrictions** section of the project overview binder.

Component (details in the components section)	Recommended to be Certified?	Reason
Software (WinEDS)	No	<ul style="list-style-type: none"> Failure to provide required State Documentation
Precinct Scanner (Insight)	No	<ul style="list-style-type: none"> Failure to provide required State Documentation
Central Count Scanner (400-C)	No	<ul style="list-style-type: none"> Failure to provide required State Documentation
DRE (Edge II w/ activator)	No	<ul style="list-style-type: none"> Failure to provide required State Documentation Paper Record not accessible to blind voters. Failure to meet state requirements for Accessibility
DRE (Edge II Plus w/ HAAT)	No	<ul style="list-style-type: none"> Failure to prove Federal Testing was conducted Failure to provide required State Documentation Paper Record not accessible to blind voters. Failure to meet state requirements for Accessibility



Sequoia Recommendation for Voting System Application:

2007-CDOS-SEQ-001-0403

Updated 04/04/08

Binary Assessment plus N/A (with conditionals)

<u>Component</u>	<u>Version</u>	<u>Accuracy</u>	<u>Security</u>	<u>Accessibility</u>	<u>Compliance</u>	<u>Testing Board Recommendation</u>
WINEDS	3.1.074	Y ³	Y ³	N/A	N ²	N
400-C w/ WINETP	3.00/1.14.3	Y ³	Y ³	Y ³	N ²	N
INSIGHT/INSIGHT PLUS w/components	HPX K1.44/APX 2.12	Y ³	Y ³	Y ³	N ²	N
EDGE II w/Card Activator	5.0.31	Y ³	Y ³	N	N ²	N
EDGE II PLUS w/HAAT	1.2.33	N ³	Y ³	N	N ^{1,2}	N

¹ Colorado Revised Statutes Title 1, Article 5, Section 6 (1-5-608.5) prohibits allowing certification of voting equipment by the Secretary of State if it has not been successfully qualified by a recognized ITA. Additionally, Rule 45.5.1.3 requires voting systems to be compliant with federal requirements.

² Missing/insufficient state documentation pursuant to Colorado Secretary of State Rule 45.

³ Provided jurisdictions follow additional procedural steps outlined in the **Conditions** section to mitigate the deficiencies of the system as evaluated. Should conditions not be applied or adhered to as indicated in this binder, the testing board would reject the system and modify the value to a "N." This is specifically addressed in the test board comments section of this binder.

Definitions:

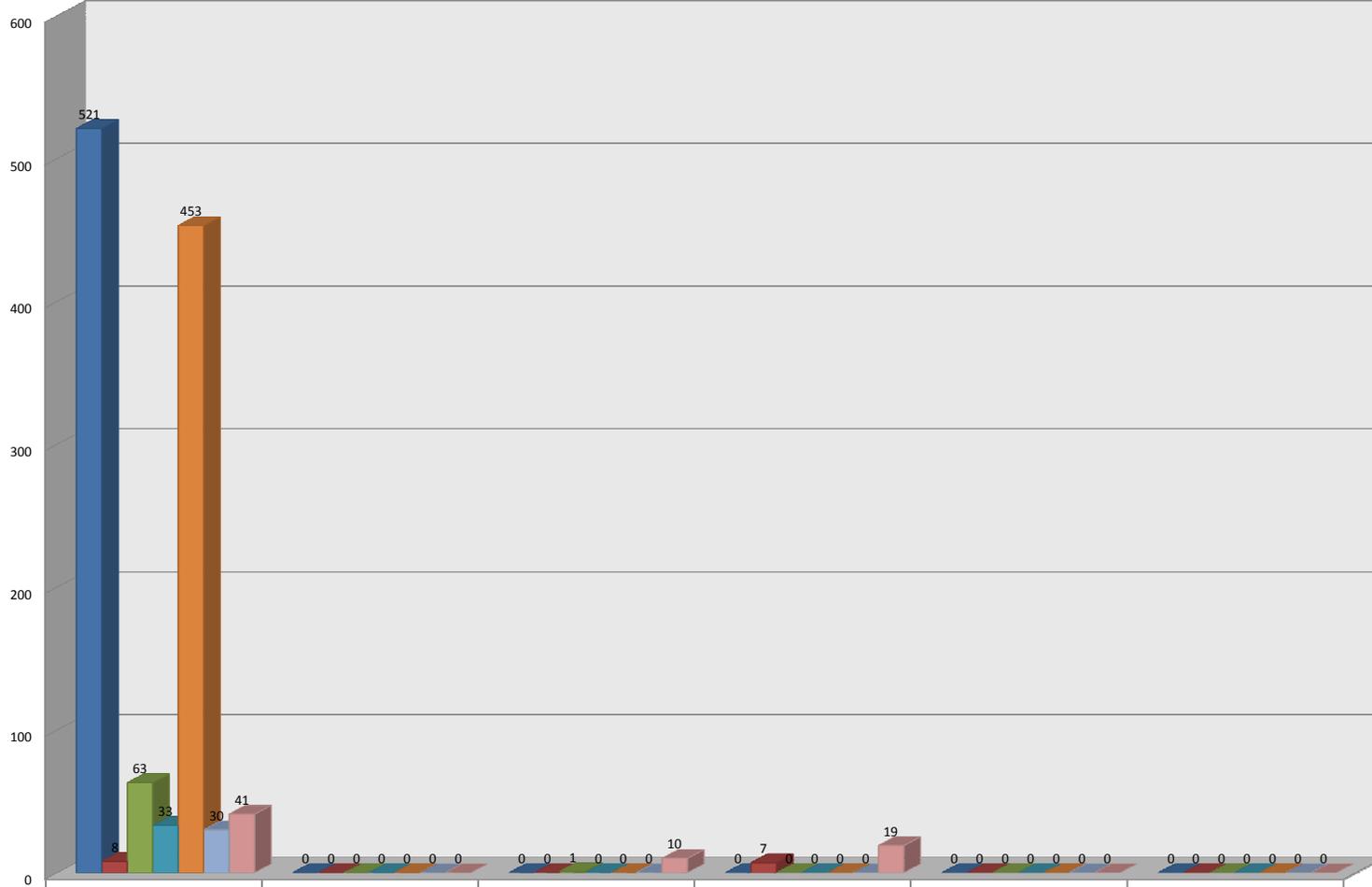
Accuracy – correctly reading, displaying, tabulating and reporting votes. (Functional, or Performance)

Security – vote data is protected and maintains integrity throughout system processing. (Audit, Security or Telecommunications)

Accessibility – voter system have requisite usability and reliability. (Functional, Accessibility, or Physical Design)

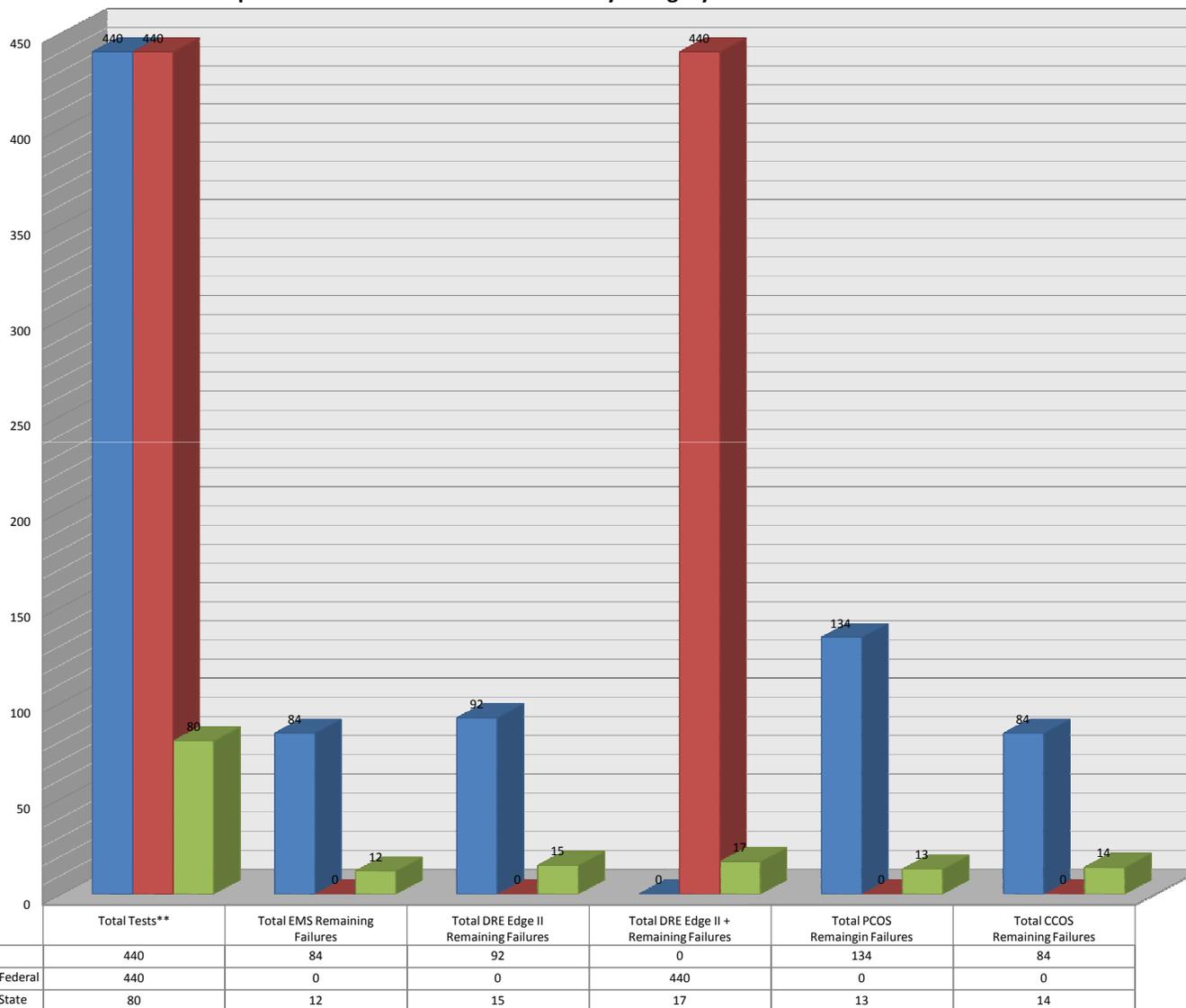
Compliance – system conforms to federal requirements for certification and/or documentation. (Documentation)

Sequoia Failure Status by Category



	Total Tests	Total EMS Remaining Failures	Total Edge II Remaining Failures	Total Edge II + Remaining Failures	Total PCOS Remaining Failures	Total CCOS Remaining Failures
Functional Requirements	521	0	0	0	0	0
Performance Levels	8	0	0	7	0	0
Physical design	63	0	1	0	0	0
Audit Capacity	33	0	0	0	0	0
Security	453	0	0	0	0	0
Telecommunications	30	0	0	0	0	0
Accessibility	41	0	10	19	0	0

Sequoia Documentation Failure Status by Category



* Incorrectly tested means the ITA either reported that a required item was not tested, or a required item was tested incorrectly for the device type.

** Total tests has N/A items removed for chart scale.

**2007-CDOS-SEQ-001-0403
PROJECT OVERVIEW BINDER “A.4”**

RESTRICTIONS



The Testing Board has identified the following items as deficient in the voting system, requiring restriction for use of the voting system components based on the review and testing of the voting system for compliance with state requirements:

Software Restrictions:

WinEDS 3.1.074

1) Documentation Requirements

Documentation was not provided by the voting system vendor to meet and test these requirements.

Rule

Text

- 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.
- 45.5.2.4.1 In addition to other documentation requirements in this rule, the voting system provider shall provide the following documents:
 - (e) A list of minimum services needed for successful, secure and hardened operation of all components of voting system.
- 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;
 - (d) Election Result Consolidation and Reporting.
- 45.5.2.6.1 All voting systems submitted for certification shall meet the following minimum system security requirements:
 - (d) The voting system shall meet the following requirements for operating system security:
 - (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;
- 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;
 - (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.

Documentation was not provided by the voting system vendor to allow testing board to evaluate this requirement.

Precinct Count Scanner Restrictions:

Insight/Insight Plus (and components)	Rule	Text
1) Documentation Requirements Insufficient documentation.	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
Documentation was not provided by the voting system vendor to meet these requirements.	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.
	45.5.2.3.2	The voting system shall meet the following environmental controls allowing for storage and operation in the following physical ranges: (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.
	45.5.2.3.19	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. (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.
Documentation was not provided by the voting system vendor to allow testing board to evaluate this requirement.	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: (i) Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals.
	45.5.2.6.3	The voting system provider shall submit to the Secretary of State its recommended policies or guidelines governing: (e) Protection abilities of a particular operating system; (f) General characteristics of supervisory access privileges; (g) Segregation of duties;

Insight/Insight Plus (and components)

Documentation Requirements continued

Documentation was not provided by the voting system vendor to allow testing board to evaluate this requirement.

Rule

45.5.2.7.10

Text

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.

Central Count Scanner Restrictions:

400-C w/WinETP

Rule

Text

1) Documentation Requirements

Documentation was not provided by the voting system vendor to meet these requirements.

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

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.

45.5.2.3.2

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.

400-C w/WinETP

Documentation Requirements continued

	Rule	Text
	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. (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.
	45.5.2.4.1	In addition to other documentation requirements in this rule, the voting system provider shall provide the following documents: (e) A list of minimum services needed for successful, secure and hardened operation of all components of voting system.
Documentation was not provided by the voting system vendor to allow testing board to evaluate this requirement.	45.5.2.6.1	All voting systems submitted for certification shall meet the following minimum system security requirements: (d) The voting system shall meet the following requirements for operating system security: (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;
Documentation was not provided by the voting system vendor to allow testing board to evaluate this requirement.	45.5.2.6.3	The voting system provider shall submit to the Secretary of State its recommended policies or guidelines governing: (f) General characteristics of supervisory access privileges; (g) Segregation of duties;
	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;

DRE Restrictions:

AVC Edge II: 5.0.31

	Rule	Text
1) Documentation Requirements Insufficient documentation.	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.
Documentation was not provided by the voting system vendor to fully meet these requirements.	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.
	45.5.2.3.2	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.
Documentation provided by the voting system vendor is inconclusive to determine the outcome of this test.	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 include documentation concerning the use of touch screen or other display and selection technology, including but not limited to: (b) Technical documentation describing the nature and sensitivity of any other technology used to display and select offices, candidates, or issues;
Documentation was not provided by the voting system vendor to allow testing board to evaluate this requirement.	45.5.2.6.3	The voting system provider shall submit to the Secretary of State its recommended policies or guidelines governing: (d) Effective password management; (e) Protection abilities of a particular operating system; (f) General characteristics of supervisory access privileges; (g) Segregation of duties;

AVC Edge II: 5.0.31

	Rule	Text
<p>Documentation Requirements continued Documentation was not provided by the voting system vendor to allow testing board to evaluate this requirement.</p>	45.5.2.7.10	<p>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:</p> <ul style="list-style-type: none">(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.
<p>2) Physical Design</p>	45.5.2.8.2	<p>Documentation of the accessibility of the voting system shall include the following items at a minimum:</p> <ul style="list-style-type: none">(c) Technology used by the voting system that prevents headset/headphone interference with hearing aids;
<p>3) Accessibility</p>	45.5.2.3.13(b) 1-5-704 35.1.5 35.1.6 35.1.8 35.1.11	<p>All DRE voting devices shall use touch screen technology or other technology providing visual ballot display and selection. The voting system provider shall include documentation concerning the use of touch screen or other display and selection technology, including but not limited to: Technical documentation describing the nature and sensitivity of any other technology used to display and select offices, candidates, or issues;</p> <p>(1) Notwithstanding any other provision of this article, each voting system certified by the secretary of state for use in local, state, and federal elections shall have the capability to accept accessible voter interface devices in the voting system configuration to allow the voting system to meet the following minimum standards:</p> <ul style="list-style-type: none">(d) Devices providing audio and visual access shall be able to work both separately and simultaneously.(e) If a nonaudio access approach is provided, the voting system may not require color perception. The voting system shall use black text or graphics, or both, on white background or white text or graphics, or both, on black background, unless the secretary of state approves other high-contrast color combinations that do not require color perception.(g) The voting system shall provide audio information, including any audio output using synthetic or recorded human speech or any auditory feedback tones that are important for the use of the audio approach, through at least one mode, by handset or headset, at high volume and shall provide incremental volume control with output amplification up to a level of at least ninety-seven decibel sound pressure level with one incremental level of eighty-nine decibel sound pressure level.(h) For voice signals transmitted to the elector, the voting system shall provide a gain adjustable up to a minimum of twenty decibels with at least one intermediate step of twelve decibels.(i) If the voting system can exceed one hundred twenty decibel sound pressure level, a mechanism shall be included to reset the

AVC Edge II: 5.0.31

Rule

Text

volume automatically to the voting system's default volume level after every use, such as when the handset is replaced, but not before. Universal precautions in the use and sharing of headsets should be followed.

(j) If sound cues and audible information such as "beeps" are used, simultaneous corresponding visual cues and information shall be provided.

Accessibility continued

37.1.4

The voting systems described in the foregoing paragraphs shall produce a record with an audit capacity for such system.

(d) The paper record shall be accessible for individuals with disabilities including non-visual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters.

45.5.2.8.1(f)

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: 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.

45.5.2.9.10

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 nondisabled voters.

AVC Edge II Plus 1.2.33

Rule

Text

1) Documentation Requirements

Insufficient federal certification compliance/documentation, i.e. 2002 VSS requirements matrix.

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.

1-5-601.5

Compliance with federal requirements. All voting systems and voting equipment offered for sale on or after May 28, 2004, shall meet the voting systems standards that were promulgated in 2002 by the federal election commission and that may thereafter be promulgated by the federal election assistance commission. Subject to section 1-5-608.2, nothing in this section shall be construed to require any political subdivision to replace a voting system that is in use prior to May 28, 2004.

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.

Documentation was not provided by

45.5.2.2.3

The voting system provider shall publish and specify processing

AVC Edge II Plus 1.2.33

the voting system vendor to fully meet these requirements.

Documentation Requirements continued

Rule

Text

standards for each component of the voting system as part of the documentation required for certification.

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.

45.5.2.3.16

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.

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.

AVC Edge II Plus 1.2.33

Documentation was not provided by the voting system vendor to allow testing board to evaluate this requirement.

Documentation Requirements continued

2) Physical Design

3) Accessibility

The Testing Board was unable to evaluate these items for this device due to errors in programming provided by the vendor that were not corrected.

Rule

Text

- 45.5.2.6.3 The voting system provider shall submit to the Secretary of State its recommended policies or guidelines governing:
(f) General characteristics of supervisory access privileges;
(g) Segregation of duties;
- 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.
- 45.5.2.8.1(f) 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: 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:
(c) Technology used by the voting system that prevents headset/headphone interference with hearing aids;
- 45.5.2.3.14(b) The voting system shall contain a control subsystem that consists of the physical devices and software that accomplish and validate the following operations:
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.
- 1-5-704 (1) Notwithstanding any other provision of this article, each voting system certified by the secretary of state for use in local, state, and federal elections shall have the capability to accept accessible voter interface devices in the voting system configuration to allow the voting system to meet the following minimum standards:
(b) The voting system shall provide a method by which electors can confirm any tactile or audio input by audio output using synthetic or recorded human speech.
(d) [35.1.5] Devices providing audio and visual access shall be able to work both separately and simultaneously.
(g) [35.1.8] The voting system shall provide audio information, including any audio output using synthetic or recorded human speech or any auditory feedback tones that are important for the use of the audio approach, through at least one mode, by headset or headset, at high volume and shall provide incremental volume

control with output amplification up to a level of at least ninety-seven decibel sound pressure level with one incremental level of eighty-nine decibel sound pressure level.

(j) [35.1.11] If sound cues and audible information such as "beeps" are used, simultaneous corresponding visual cues and information shall be provided.

(n) Audio ballots shall meet the following standards:

(III) The elector shall be able to determine how many candidates may be selected for each office.

(IV) The elector shall have the ability to verify that the physical or vocal inputs given to the voting system have selected the candidates that the elector intended to select.

(V) The elector shall be able to review the candidate selections that the elector has made.

(VI) Before casting the ballot, the elector shall have the opportunity to change any selections previously made and confirm a new selection.

(VII) The voting system shall communicate to the elector the fact that the elector has failed to vote for an office or has failed to vote the number of allowable candidates for an office and require the elector to confirm his or her intent to undervote before casting the ballot.

(IX) The elector shall have the opportunity to input a candidate's name for each office that allows a write-in candidate.

(X) The elector shall have the opportunity to review the elector's write-in input to the voter interface device, edit that input, and confirm that the edits meet the elector's intent.

(XI) The voting system shall require a clear, identifiable action from the elector to cast the ballot. The voting system shall explain to the elector how to take this action so that the elector has minimal risk of taking the action accidentally, but when the elector intends to cast the ballot, the action can be easily performed.

(XII) After the ballot is cast, the voting system shall confirm to the elector that the ballot has been cast and the elector's process of voting is complete.

(XIII) After the ballot is cast, the voting system shall prevent the elector from modifying the ballot cast or voting another ballot.

Accessibility continued

34.5 If a political subdivision acquires a new voting system, the system must be accessible to persons with physical, cultural/educational, mental/cognitive disabilities and provide the voter in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters.

35.1.2 The voting system shall provide a method by which voters can confirm any tactile or audio input by having the capability of audio output using synthetic or recorded human speech, which is reasonably phonetically accurate.

AVC Edge II Plus 1.2.33

Rule

Text

37.1.4 The voting systems described in the foregoing paragraphs shall produce a record with an audit capacity for such system.
(d) The paper record shall be accessible for individuals with disabilities including non-visual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters.

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 nondisabled voters.

3) Performance

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.
(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.

**2007-CDOS-SEQ-001-0403
PROJECT OVERVIEW BINDER “A.4”**

CONDITIONS



FINAL – 4/4/2008

Conditions for Use – SEQUOIA - AMENDED 4/4/08

The Testing Board would also recommend the following conditions for use of the voting system. These conditions are required to be in place *should* the Secretary approve for certification any or all of the items indicated in the **COMPONENTS** section. The Testing Board has modified the conditions based on information provided through public hearing under legislative updates to consider additional procedures. Any deviation from the conditions provides significant weakness in the security, auditability, integrity and availability of the voting system.

Global Conditions (applies to all components):

- 1) Modem and other telecommunication devices may not be used on any subsystem component - system provider was unable to meet or provide prerequisite FIPS 140/180 certifications.
- 2) Provisional ballots must be processed separately from non-conditional ballots - system subcomponents are unable to functionally differentiate and correctly process to Colorado specific requirements.
- 3) Coordination of Escrow Setup - Upon Certification, voting system manufacturer must coordinate the Escrow of the TRUSTED BUILD software with SOS escrow, or third party escrow service as required by Rule 11 prior to use in Colorado.
- 4) Abstract Report Generation - abstracts used for State reporting must come from WinEDS Software, or other external solution, rather than from the specific device.
- 5) Trusted Build Verification (all software and firmware components)
 - a) The system components do not allow for proper verification of trusted build software. Any breach of custody and/or other security incidents will require the rebuild of the component with the state trusted build software. This requirement applies to all voting devices, firmware and software components of the system.
 - b) Counties shall ensure that hardware, software and firmware purchased for use of the system matches the specifications of VSTL/EAC and/or State Certified and trusted versions, not to the version presented in the vendor documentation.
- 6) Counties using the voting system shall testify through their security plan submission that the voting system is used only on a closed network.

Software Conditions (WinEDS 3.1.074):

- 1) System/Database/Network Security Hardening.
 - a) Because the voting system operates in a non-restricted system configuration containing open file system access to locate, copy, open and overwrite without detection, election vote content database files outside of election management system application by third-party tools, counties will be required to modify their physical environmental conditions, or work with current Sequoia documentation (not currently tested) and request variance from the Secretary of State to use Sequoia hardening documentation in lieu of environmental changes. Counties shall submit their plan for approval to the Secretary of State's office to be included in the County Security Plan on overcoming these conditions through county environmental and/or procedural changes where possible.
 - b) In addition to physical environmental changes, counties shall maintain the integrity of the master WinEDS databases with one of the following two methods:
 - Option #1 - Create a second (or backup) copy of the WinEDS database that is created immediately after the point of memory card downloads. The backup copy shall be stored on closed CD Media and documented as matching the master database. This process shall be observed by two election staff members. Chain of custody documents shall be generated for the media, and the media shall be sealed with at least two tamper evident seals and stored in a sealed or lockable transfer case that is stored in a limited access area. On election day, the designated election official shall load the sealed copy of the database onto the server and proceed with uploading memory cards after documenting the loading of the backup master database onto the system. After loading the sealed database copy, the county shall re-secure the database with seals (updating necessary logs) in the limited access location; or
 - Option #2 - Create a second (or backup) copy of the WinEDS database that is created immediately after the point of downloading all memory cards. The copy of the database will be escrowed with the Colorado Secretary of State's office along with the "profile" database. After each of the events described below, the county shall provide both an updated copy of the database to the Secretary of State's office, an updated SQL and WinEDS audit log, and the forensic analysis of the SQL databases (both profile and election databases) performed by a commercially available forensics tool, identifying changes to database properties since the last report. Events triggering a report update to the Secretary of State include: any download of memory cards, any upload of memory cards, completion of L&A Testing, And COMPLETION of Post-Election Audit. Reports are to be submitted to the Secretary of State's office within 24 hours of the event.

Counties shall indicate in their Security Plan which option they will be executing to meet the security requirements.

- c) Additionally, to overcome deficiencies in security and auditing of the system, the county will be required to perform increased Election Night and Post Election Audits for this system. All post-election audit data shall process a hand count of paper ballots which shall match the totals report from the specific device, as well as the totals for the WinEDS database. Counties shall prepare for this event with one of two methods:

Option #1 – Prepare for the upload of memory cartridges as normal. Print necessary zero report. Upon uploading each individual memory card, print a summary report showing the change in totals from the upload of the memory card. Label the report to match the name/number of the memory card uploaded. Continue to upload memory cards and print totals reports to match. When auditing a specific device, use the difference between the report totals for the memory card selected for the audit and the totals from the immediately preceding memory card report to calculate vote totals generated by the WinEDS software.

When memory cards are delivered to the county for upload, the machine generated report shall be delivered for inspection as well. During the post-election audit, when the summary report indicated above is created, the difference totals (delta report) are compared to the totals from the report generated by the device at the polling place. If the reports match, the public is ensured that the totals from the polling place match the totals from the county server. If the totals are different, the county is to report the situation to the Secretary of State's office for audit, security and remedy procedures.

During the post election audit process, the totals of the paper record for the specific device are to be hand counted and verified against the electronic record for the device. The canvass board shall report the verification of three totals to match – the paper record of the device, the totals of the electronic vote on the device, and the totals in the central count server; OR

Option #2 – Prepare for the upload of memory cartridges by creating one master default database (containing all memory cards/cartridges). Create individual databases to contain values (upload data) for each separate memory card (or in some instances by batch of ballots – see condition #4b under Central Count devices. Upload memory card/cartridges into master database, and into the specific database created for that memory card (two separate uploads). This process can take place any time after the close of polls including through the canvass period, with observation by at least two people. Election summary reports shall be printed from each individual database and manually added together. The totals from the individual databases must match the master database before proceeding. Upon verification that the master and individual databases match, the county can then use the individual reports to conduct a hand count of the paper ballot (or paper record) generated by the device to show that the WinEDS totals match. The verification of the separate upload databases verify that the database totals match the field totals on each memory card device, as was designed after the point of Logic and Accuracy testing took place.

2) Audit Trail Information.

a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing by other methods.

b) Operators of the system shall also be required to maintain logs indicating use of the report printing functions of the software, and detailed information to changes of the system including hardware changes which shall include: insert removable media, remove removable media, modify system hardware drivers, modify system physical hardware, and any other system property changes made by either judges or other trusted staff. Logs shall be maintained physically in a file outside or separate from the database, which is NOT accessible for review and/or modification by user/operator accounts on the system, but that is readily accessible to election officials or other interested party.

3) Trusted Build Protection.

Applies to WinEDS software and custom components of SQL server as applicable. Refer to Global Condition #5a for ensuring integrity of trusted build.

4) Performance Deficiencies.

Due to failures in performance, counties shall allow extra time for downloads and uploads of memory card devices. This may impact programming, testing and use of the system on election night. Counties shall ensure trusted staff is properly trained on this issue and accommodating the allowable time required for programming memory devices.

5) Provisional Ballots.

The software is not capable of processing provisional ballots internally to accept federal and state only questions. A procedure outside of the voting system will be required. Additionally, the abstracts and reports created by the software do not meet the requirements of rule 41.6.3(g) and users of the system will be required to generate an abstract outside of the voting system.

6) Election Database Creation and Testing.

The system relies heavily on an external program called BPS which typically is used for importing the ballot setup process into WinEDS. Since this program is to be considered non-trusted and is not third party as it is made by the voting system manufacturer, the program shall only be able to receive data from WinEDS. WinEDS shall not be used to import data from BPS, unless the data is in a static import file format such as a flat file, csv, txt, or similar which can be imported without the use of vendor proprietary software. Additional testing will therefore be required by counties for both electronic and paper ballots to ensure all voting positions are working as designed prior to each election. This shall include ordering a complete set of at least 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

Precinct Count Scanner Conditions (Insight/Insight Plus):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

2) External Power Supply Required

The device contained internal power to run for three hours, however under the internal battery included with the system, the device did not count votes correctly. Using an external power source such as a UPS unit providing battery power allows the device to meet the power requirement and count correctly. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for each component.

3) Device Security Accessibility.

- a) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) person entry with detailed logs.

b) County use of voting system will require use of WinEDS Software to modify the “administrator” password on the voting device.

4) **Ballot/Race Conditions Simulation.**

Additional County testing shall be required to accommodate ballots with conditions from each election. This shall include ordering a complete set of at least 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

5) **Audit Trail Information:**

- a) Operators of the system shall also be required to maintain logs indicating use of the administrator functions of the device by either judges or other trusted staff.
- b) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing by other methods.
- c) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper ballots to match the totals generated from the WinEDS software as indicated in Software condition #1c.

6) **Voting Secrecy.**

Insufficient privacy of ballot was detected using secrecy sleeve. Election administrators must ensure system secrecy sleeve (from Sequoia) is used for ballots up to 14". For longer ballots, the counties shall create a secrecy sleeve to accommodate the deficiency and submit design form to Secretary of State for approval.

Central Count Scanner Conditions (400-C):

1) **Intrusion Seals for Protection of Trusted Build Firmware.**

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated. Refer to Global Condition #5a for ensuring integrity of trusted build.

2) **System/Database/Network Security Hardening.**

Because the voting system operates in a non-restricted system configuration containing open file system access to locate, copy, open and overwrite without detection, election vote content database files outside of election management system application by third-party tools, counties will be required to modify their physical environmental conditions, or work with current Sequoia documentation (not currently tested) and request variance from the Secretary of State to use Sequoia hardening documentation in lieu of environmental changes. If approved, counties shall submit plans for approval to the Secretary of State's office on overcoming these conditions through one of the two stated processes.

3) **External Power Supply Required.**

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the

component. Acceptable power supply sources include generators and other facility based solutions.

4) Audit Trail Information:

a) Judges shall be required to include device serial number on all reports regarding use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

b) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include a hand count of at least the following amount of ballots counted on the device for the specific races selected in the post election audit:

Total # of Ballots Counted on Device:	Total # of Ballots to audit:	# of errors requiring escalation:
150,000 to 500,000	1,250	6
35,001 to 150,000	800	4
10,001 to 35,000	500	3
3,201 to 10,000	315	2
1,201 to 3,200	200	2
501 to 1,200	125	2
281 to 500	80	1
151 to 280	50	1
91 to 150	32	1
51 to 90	20	1
26 to 50	13	1
16 to 25	8	1
9 to 15	5	1
1 to 8	3 or 100% if less than 3	1

Errors detected during the manual audit process shall be resolved according to C.R.S. 1-7-514, and Secretary of State Rule 11. Errors discovered exceeding the error rate identified in the table above shall require escalation measures including increased audits as prescribed by the Secretary of State’s office. County officials shall contact the Secretary of State’s office as soon as possible if an audit detects errors above the escalation threshold.

The verification of the hand count of paper ballots shall match the totals generated from the WinEDS software as indicated in Software condition #1c. Counties shall load only the master database from the secured storage location for processing the post election audit ballots as indicated in Software Condition #1b. Counties shall prepare database and batches of ballots prior to scanning into system (for election results) to accurately generate reports in batch sizes as necessary for the audit.

c) Additional County testing shall be required to accommodate ballots with conditions listed. This shall include ordering a complete set of at least 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

5) Device Security Accessibility.

Device level administrative functions requiring access involving the use of keys, memory cards, and

passwords must be restricted to no more than two (2) person entry with detailed logs.

DRE Conditions (Edge2):

1) External Power Supply Required.

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component to accommodate a 90 minute short coming experienced by the Testing Board during testing of the device.

2) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

3) Ballot/Race Conditions Simulation.

Additional County testing shall be required to accommodate ballots with conditions listed. This shall include ordering a complete set of at least 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly. All ballots in this detail shall be "marked" using the DRE device as applicable for similar testing.

4) V-VPAT Paper Record Shall be Handled per Rule 11.6.

- a) Prescribed paper record is of the thermal type and requires special storage conditions to avoid legibility degradation. Counties shall follow the requirements for handling according to Secretary of State Rule 11 and 43.
- b) Election judges are required to perform the "Printer Test" in between paper changes and verify with one additional judge that the paper has been loaded correctly and is printing according to design which ensures that all machines will have paper records for each vote cast.

5) V-VPAT Security.

The V-VPAT device provides no assurance that it cannot accommodate other devices, and/or the device is a standard communication port. This connection between the V-VPAT printer and the DRE unit shall be secured with tamper evident seals with proper chain of custody documentation to prevent and detect tampering.

6) Accessible Distances.

Operators of the system shall be required to provide an accessible solution by operating the device on a separate table. The manufacturer's stand does not meet accessible reaches as outlined in 1-5-704. Counties shall be educated on these measurements and ensuring that the table top solution complies with the requirements. This condition could also be achieved with the use of a reach stick that is at least 4" in length. Should the counties use the DRE in the stand with a reach stick, the counties shall ensure that a side approach by a wheelchair is possible due to the deficiencies in the knee clearance (depth and width) of the stand.

7) Accessible Operation.

Due to the inability for the voter to pause and resume the audio text, election judges shall provide instructions specific to this fact to the voters and operations for repeating the text if text was missed, which shall include details on navigating forward and backwards through the system prompts.

8) Audit Trail Information:

- a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing by other methods.
- b) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper records to match the totals generated from the WinEDS software as indicated in Software Condition #1c.

9) Confusing Instructions to Voters.

Due to the complicated messaging provided to voters during the V-VPAT review process, the use of the device shall require election administrators to change the wording of the review screen to properly indicate to voters that a review of the ballot is taking place.

10) Device Security Accessibility.

- a) The “override.ini” file is not a VSTL-certified file, and poses the potential for a security threat (denial of service in particular). Due to this fact, the State will require the creation of a State copy of the file to ensure change control and associated hash values are passed to the counties through the distribution of the trusted build. Should a county request a change to the State certified copy of the file, the change will be made and the State will record new hash values for the file which will then be deployed in a similar fashion as the trusted build to the counties.
- b) Devices deployed in Colorado shall require a “lockable” activate button. Voter activation by use of the activate button shall not be used in the voting environment.
- c) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) person entry with detailed logs.

DRE Conditions (Edge2plus):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

2) Ballot/Race Conditions Simulation.

Additional County testing shall be required to accommodate ballots with conditions listed. This shall include ordering a complete set of at least 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly. All ballots in this detail shall be "marked" using the DRE device as applicable for similar testing.

3) V-VPAT Paper Record Shall be Handled per Rule 11.6.

- a) Prescribed paper record is of the thermal type and requires special storage conditions to avoid legibility degradation. Counties shall follow the requirements for handling according to Secretary of State Rule 11 and 43.
- b) Election judges are required to perform the “Printer Test” in between paper changes and verify with one additional judge that the paper has been loaded correctly and is printing according to design which ensures that all machines will have paper records for each vote cast.

4) V-VPAT Security.

The V-VPAT device provides no assurance that it cannot accommodate other devices, and/or the device is a standard communication port. This connection between the V-VPAT printer and the DRE unit shall be secured with tamper evident seals with proper chain of custody documentation to prevent and detect tampering.

5) Accessible Distances.

Operators of the system shall be required to provide an accessible solution by operating the device on a separate table. The manufacturer’s stand does not meet accessible reaches as outlined in 1-5-704. Counties shall be educated on these measurements and ensuring that the table top solution complies with the requirements. This condition could also be achieved with the use of a reach stick that is at least 4” in length. Should the counties use the DRE in the stand with a reach stick, the county shall ensure that a side approach by a wheelchair is possible due to the deficiencies in the knee clearance (depth and width) of the stand.

6) Accessible Operation.

Due to the inability for the voter to pause and resume the audio text, election judges shall provide instructions specific to this fact to the voters and operations for repeating the text if text was missed, which shall include details on navigating forward and backwards through the system prompts.

7) Audit Trail Information:

- a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing by other methods.
- b) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper records to match the totals generated from the WinEDS software as indicated in Software Condition #1c.

8) Confusing Instructions to Voters.

Due to the complicated messaging provided to voters during the V-VPAT review process, the use of the device shall require election administrators to change the wording of the review screen to properly indicate to voters that a review of the ballot is taking place.

9) Device Security Accessibility.

- a) The “override.ini” file is not a VSTL-certified file, and poses potential for security threat (denial of service in particular). Due to this fact, the State will require a State copy of the file ensuring change control is passed to the counties through the distribution of the trusted build. Should a county request a change to the State certified copy of the file, the change will be made and the State will record new hash values for the file which will then be deployed in a similar fashion as the trusted build to the counties.
- b) Devices deployed in Colorado shall require a “lockable” activate button. The voting system

vendor must provide schematics and assembly drawings of the button prior to installation and use, which must be approved by the Secretary of State prior to deployment. Voter activation by use of the activate button shall not be used in the voting environment.

c) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) person entry with detailed logs.

Insight Memory Pack Receiver Conditions (2.1.5):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on memory cartridge & memory pack reader/burner and will require additional seals for protection against entry points as indicated by the Secretary of State. Requirements apply to physical MPR and all data cartridges used by the county. Refer to Global Condition #5a for ensuring integrity of trusted build.

Card Activator Conditions (Version 5.0.31):

1) Intrusion Seals for Protection of Trusted Build Firmware

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on device and will require additional seals for protection against entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

2) Cross Compatibility

The Testing Board has determined that the Card Activator is compatible for use with either the Edge2 or Edge2plus DREs

HAAT Model 50 Conditions (Version 2.1.18):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on device and will require additional seals for protection against entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

2) Cross Compatibility

The Testing Board has determined that the HAAT is compatible for use with either the Edge2 or Edge2plus DREs.

**2007-CDOS-SEQ-001-0403
PROJECT OVERVIEW BINDER “A.4”**

COMMENTS



Testing Board Comments (updated – A.4)

Changes to the project overview binder reflect predominantly changes allowed to conditions pursuant to SB08-1105. The Testing Board has reflected conditional changes throughout this version of the document.

Testing Board Comments (updated – A.3)

In addition to other changes to the Project Overview Binder, the Testing Board would like the opportunity to note that the Executive Summary report was not developed independently by the Testing Board.

Testing Board Comments (original)

The Testing Board has unveiled a known reality that no computer system is perfect. Additionally, we have discovered and documented that no system can currently meet the requirements of Rule 45 as applied in its strictest sense. Where possible, the Testing Board attempted to overcome these deficiencies in the form of “conditions for use” of the system – procedural workarounds.

The Testing Board recognizes that the conditions created are in essence a “last resort” workaround to accommodate requirements that do not meet specific sections of Colorado Revised Statutes 1-5-615. The preference of the Testing Board would be to have the specific deficiencies addressed with a system solution as required. Given the ability to mitigate deficiencies with procedural workarounds (C.R.S. 1-5-621), the Testing Board presents conditional use scenarios in the “**Conditions**” section that are directly tied to the recommendation status. Being that many workarounds address the security, auditability and availability of the system component, the Testing Board would firmly reject any option which removes, replaces or diminishes the conditional requirement and still allow the system to be used and recommended for certification. Any “Y” value in the **Recommendation** table would change to a “N” value with any change to the conditions.

These conditional procedures rely heavily on proper execution by county administrators and/or election judges. While we have faith that these dedicated workers will attempt to perform their duties to the best of their abilities, a majority of the conditions involve a human element which may or may not produce the acceptable outcome. This single factor alone causes concern that a security issue may not be resolvable in a post-election scenario.

Finally, it is of value to point out that the conditions that address security specific events are only addressing the attack scenario of a change in vote totals (refer to Cyber Security Report). The essence of the workaround in this case is to ensure that the vote totals calculated electronically are a match to the paper records. This requires absolute assurance that all paper records exist and are auditable for a successful outcome and high confidence in the report of votes by any given county.