

State of California

USE PROCEDURES

Dominion Voting Systems Corporation for Premier branded products

These procedures are proposed for adoption by the California Secretary of State pursuant to Elections Code sections 19200 and 19205 and shall regulate and govern the use of Premier Election Solutions AccuVote®-OS and AccuVote®-TS (Touch Screen) at all elections governed by the California Elections Code.

These procedures shall be effective upon approval by the Secretary of State and shall be used in conjunction with all other statutory and regulatory requirements. Insofar as feasible, all procedures prescribed herein shall be carried out in full view of the public.

These procedures constitute a minimum standard of performance. They are not intended to preclude additional steps being taken by individual election officials to enhance security and reliability of the electoral process.

Submitted

October 23, 2008

Revised September 13, 2010 to add audit log management information
Revised October 19, 2010 to remove “confidential and proprietary” notation



Table of Contents

Table of Contents	2
1.1. System Description and Components	4
1.2 Terms and Definitions	7
2 Ballot Definition	
2.1. Overview	17
2.2. Paper and Printing Specifications	17
2.3. Layout Requirements and Specifications	17
3 System Installation and configuration	
3.1. Hardware Requirements and Specifications	18
3.2. Hardware and Network Setup and Configuration	18
3.3 Software and Firmware Upgrades	19
3.4. Acceptance Testing	20
4 Election Setup and Definition	
4.1 GEMS System	22
4.2 AccuVote-OS Testing	23
4.3 AccuVote-TSX Testing	26
4.4 AccuVote-OS and AccuVote-TSX Audit Log Retention	30
4.5 Public Logic and Accuracy Board and Certification of Testing	30
4.6 Ballot Tally Programs	30
4.7 Election Observer Panel	31
5 Polling Place Procedures	
5.1 Precinct Supplies, Delivery and Inspection	32
5.2 Polling Place Setup	33
5.3 Opening the Polls	34
5.4 Polling Place Procedures	34
5.5 Special Needs Voters	37
5.6 Provisional Voters	38
5.7 Closing the Polls and Vote Reporting	38
5.8 Securing Audit Logs and Backup Records	40
5.9 Troubleshooting and Problem Resolution	40
6 Absentee/Mail Ballot Procedures (central tabulation)	
6.1 System Startup and Pre-Tabulation Report Procedures	46
6.2 Tabulation Procedures	46
6.3 Post Tabulation Report and Shutdown Procedures	47
7 Semi-Official Canvass Tabulation and Reporting	
7.1 System Start-Up and Pre-Tabulation Reports	48
7.2 Processing Vote Reports	50
8 Official Canvass and Post-Election Procedures	
8.1 Election Observer Panel	51
8.2 Canvassing Precinct Returns	51
8.3 Canvassing Absentee Returns	53
8.4 Canvassing Provisional Ballots	54
8.5 Canvassing Write-In Votes	54
8.6 1% Manual Tally	55
8.7 Handling Ballot Exceptions	55
8.8 Post Election Logic and Accuracy Testing	56
8.9 Final Reporting of Official Canvass	56
8.10 Backup and Retention of Election Material	56
9 Recount procedures	58
10 Security	
10.1 Physical Security of System and Components	60

10.2 Logical Security of System and Components	67
10.3 Security Procedures for Central Processing	69
10.4 Security Procedures for Polling Place	70
10.5 Audit Trails	70
10.6 Audit Logs – AccuVote OS	70
Reference Materials	82
Appendix A – Audit Log Management for TS and TSx units	83

Introduction

1.1. System Description and Components

This manual of USE procedures is for jurisdictions using the Premier Election Solutions, Inc. (Premier) systems as certified by the State of California. It is to be used in conjunction with the user guides distributed at the time of upgrade. Additional copies, if needed, may be obtained from Premier. The system components are listed below:

- *GEMS® Software Version 1.18.24*
- *AccuVote®-TSX Ballot Station Version 4.6.4*
- *Key Card Tool Version 4.6.1*
- *Voter Card Encoder Version 1.3.2*
- *VC Programmer 4.6.1*
- *AccuVote®-OS firmware version 1.96.6*
- *AccuVote®-OS Central Count firmware version 2.0.12*
- *AccuFeed*

An overview of each component follows:

The Global Election Management System (GEMS)® 1.18.24 Election Management System is a Microsoft Windows -based election management and tabulation software that allows complete control of the election process, from precinct/district set-up, to race definition, tabulation and reporting. With GEMS software you can combine the programming of absentee or mail ballots and create the ballot layout of the optical scan and touch screen units all in one programming process. GEMS 1.18.24 software completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N-1-06-22-22-001.

The Ballot Station Software firmware 4.6.4 is designed to run exclusively on the Premier AccuVote®-TSX touch screen voting device with the AccuView Printer® Module (AVPM). This software allows a voter to interact with the voting device by touching the unit's touch screen panel for the capture of their vote. The Ballot Station software 4.6.4 incorporates changes from previous releases to utilize the AVPM.

The Key Card Tool 4.6.1 is a PC based software application designed to enhance the security provided by the AccuVote-TSX units used in an election. The Key Card Tool application, when used in conjunction with an external smart card reader device, allows the user to create a smart card encoded with user-defined security codes or keys. The Key Card may be used to encode the security key values on the election's smart card reading equipment. These values can be changed per election. The Key Card Tool 4.6.1 version completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N-1-06-22-22-001.

The Voter Card Encoder 1.3.2 is a device designed to encode voter access cards for the purpose of activating ballots on the AccuVote-TSX units used in an election. The Voter Card Encoder is encoded with "Master" voter access cards created from the AccuVote-TSX Ballot Station database application. The Voter Card Encoder can be pre-programmed with up to eight different ballot styles. Poll workers can encode voter access cards for each voter with the appropriate ballot style in their voting location. The Voter Card Encoder 1.3.2 completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N-1-06-22-22-001.

The VCPprogrammer 4.6.1 is a PC based application that, when used with an external smart card reading device, can be used to create voter access cards for use on AccuVote-TSX Ballot Station units configured for an election.

A file exported from the GEMS election database supplies the information required by the application to create voter access cards. When this file has been made available to VCPprogrammer, the application can be used to identify the precinct and party associated with the ballot to be copied onto a voter access card for a voter.

VCPprogrammer may be configured to interface with a voter registration system during a live election. When configured this way, the application automatically identifies the precinct and party associated with the ballot to be copied onto a voter access card when voter information is updated in a file generated by the registration system and referenced by VCPprogrammer. The VCPprogrammer 4.6.1 completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N-1-06-22-22-001.

The AccuVote®-OS Optical Scan (model D) with 1.96.6 firmware is a mark sense paper-based voting device. It offers a precinct count and absentee voting solution that can be configured as a stand-alone system in a polling environment. Each precinct count AccuVote-OS unit is loaded with a memory card programmed with ballot information for the corresponding polling location or precinct(s). The results of ballots scanned by the AccuVote-OS are tallied to the memory card, and these results are uploaded to the host computer at the close of election. The AccuVote-OS will accommodate three different size ballots, all 8 ½ X 11", 14", and 18" ballots in length. Ballots can be fed into each unit in any direction or orientation. Both sides of the ballots will be read and recorded at the same time. The AccuVote-OS also has the option of being programmed to reject any over-voted, fully blank ballot or under-voted races if required by the State. The AccuVote-OS (model D) with firmware version 1.96.6 completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N-1-06-22-22-001.

AccuVote-OS Central Count firmware 2.0.12 is a compact and, scaleable batch ballot processing solution employing the AccuVote-OS ballot counting device configured with a Central Count firmware, linked over a local area network connection to the GEMS election management server. Ballots scanned by the AccuVote-OS Central Count unit pass card ID information to the GEMS server over the local network. The GEMS server confirms the ballot identification, and returns a ballot mask to the AccuVote-OS Central Count device. Using the ballot mask, valid voting positions are uploaded for the ballot to GEMS.

The AccuVote-OS Central Count is used for processing large volumes of mail ballots, such as absentee ballots. Since the ballot information as well as the tally files is stored on the GEMS server, central count does not limit the number of unique ballot styles processed in a single processing session. AccuVote-OS Central Count mode allows any ballot type to be fed into the AccuVote-OS without any presorting of ballots. All that is required is that the vote center in which ballots are counted is logically associated with all the election precincts to the vote center in the GEMS software database.

AccuVote-OS Central Count may be configured with multiple AccuVote-OS Central Count units linked to the GEMS server in either a local area network configuration or using Windows Remote Access Server (RAS).

The AccuVote-OS Optical Scan Central Count 2.0.12 completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N1-06-22-22-001.

The AccuFeed Ballot Feeder is a mechanical ballot feeding device which can be used with the AccuVote-OS. This hardware allows the operator to place stacks of ballots into the input

stacker tray which are fed into the AccuVote-OS optical scan unit. The AccuFeed ballot feeder does not tabulate or scan the ballot. The unit functions to feed the next ballot to the AccuVote-OS unit. The AccuFeed ballot feeder is placed on top of the AccuVote-OS in the Central Count configuration and the ballot feed function is controlled by the AccuVote-OS via a single optical coupler.

1.2 Terms and Definitions

This section contains a comprehensive glossary of terms used with the AccuVote-OS, the AccuVote-TSX, and related functions in GEMS, in alphabetical order.

“Absentee Voter”

A voter who votes at a location other than their polling place by means of paper ballot, or by means of an electronic ballot at the election office or a designated satellite location.

“AccuVote Server”

The console window used in GEMS for programming AccuVote-OS and AccuVote-TSX election media and uploading election results.

“AccuVote-OS”

The AccuVote-OS (AVOS) unit consists of optical scanner hardware and software that accepts and tallies votes, prints reports, and rejects votes based on specified conditions (e.g., overvotes, blank voted ballots)

“AccuVote-TSX”

The AccuVote-TSX (AVTSX) unit consists of hardware and software for the electronic ballot station functions, which includes the selection of the ballot, the detecting and recording voter choices, and the printing of reports. Additionally, the AVTSX prints out a voter verifiable paper trail on the AccuVote Printer Module (AVPM) for a voter to review the voted selections prior to casting a ballot on the AVTSX.

“Accessible Voter Verifiable Printed Audit Trail (AVVPAT)”

The Accessible Voter Verifiable Paper Audit Trail refers to the AccuView Printer Module's (AVPM) printed summation of a voter's choices that the voter verifies against the electronic ballot.

“Administrator Card”

A special smart card programmed to allow complete access to all functions on the AccuVote-TSX ballot station. It is NOT intended for poll worker use and is NOT needed for closing the polls and for initiating the printing of election results.

“Administration Screen”

The various functions of the administrative window on the AccuVote-TSX designed only to be accessed at specified points in the election process. Functions on this screen include: Start Election, End Election, Transfer Polling Data, Exit Administrative State, and Shutdown System.

“Archive”

Election and election results files preserved for back-up or election recovery purposes.

“Archiving of Election Data”

Once the transport media results have been entered on the host, the removable disk is archived. Verification of tabulations can be re-created by comparing records from the fixed storage on the AccuVote-TSX with the results from the transport storage on the disks.

“Audio Ballot”

The ballot composed in audio format, containing identical race and candidate content and ordering as the corresponding visual ballot, and including operational instructions for the selection of candidates and ballot measures, traversing the race list, definition of write-in candidates, and printing and casting of ballots.

“Audit Log” An audit record of the audit transactions on the AccuVote-OS and the AccuVote-TSX. The audit log provides the supporting documentation for verifying the correctness of the reported results. The audit function presents a record of all system activity.

“AccuView Printer Module (AVPM)”

The AccuView Printer Module (AVPM) that attaches to the AccuVote-TSX unit for printing the Accessible Voter Verifiable Paper Audit Trail (AVVPAT).

“Backup Flash Memory”

The internal “flash” memory storage location on the AccuVote-TSX, where elections and election results are stored.

“Ballot”

A ballot refers to a rotated ballot style.

“Ballot ID”

A unique identifier number assigned to the ballot.

“Ballot Serial Number”

A unique serial number identifying a voted AccuVote-TSX ballot.

“Base Precinct”

Any largest area of a jurisdiction not intersected by district boundaries.

“Ballots Cast” The total number of ballots cast on either an individual AccuVote-TSX or at a polling location, or on the GEMS host accumulation/reporting system.

“Ballot Station Software”

A single integrated software program residing on the AccuVote-TSX motherboard that displays, processes, reports, and transfers electronic ballot information.

“Blank Voted”

A ballot with no voter selections in any race, question, or issue.

“Button”

An object on the GEMS or the AccuVote-TSX user interface which is touched in order to activate a function.

“Candidate” An individual running for office, for whom voters have the opportunity to vote on a ballot.

“Cast Ballot Button”

Button that is touched when the voter wishes to cast their ballot after all desired selections have been made and verified on the AVPM..

“Challenge Board”

The function used to review challenged / provisional ballots.

“Challenged or Provisional Ballot” A ballot corresponding to a voter whose right to vote at a polling location has been challenged or a voter who insists that they be allowed to vote at the polling place in question. Challenged or provisional ballots are reviewed by jurisdiction administration prior to being released for counting or rejection.

“Copy”

The number of times a memory card or election media has been programmed without ballot layout having changed.

“Count” A field display on the AccuVote-TSX to indicate either the number of ballots counted in the current election, or the total number of ballots counted since the manufacture of the AccuVote-TSX. The first is an Election Count and the second count is a System Count.

“Current Candidate”

The candidate currently selected on either the visual or audio ballot.

“Current Race”

The race containing the current candidate or ballot measure.

“Central Tabulating System”

Also referred to as GEMS. The computer system that reads the votes from the AccuVote-OS and AccuVote-TSX removable media, then tabulates the votes from all polling places (either satellite, central or precinct locations).

“Closed Primary”

An optional ballot criterion for conducting primary elections in which voters affiliated with a particular party may vote only for that party’s candidates.

“Contest”

The aggregate of candidates who run against each other for a particular office, or ballot measures.

“Dynamic Host Configuration Protocol (DHCP)” Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a DHCP server to automatically assign an IP address to an individual computer’s TCP/IP software. DHCP assigns a number dynamically from a defined range of numbers (i.e., a scope) configured for DNS servers or WINS servers.

“Download” The programming of election and ballot information onto the removable storage media for the AccuVote-OS and AccuVote-TSX.

“Election Counter”

The total number of ballots cast on an AccuVote-TSX during a specific election. Also known as the Public Counter.

“Election Name”

The name of the election programmed to election media.

“Electronic Ballot”

The electronic ballot is displayed with the appropriate candidates and issues presented on a touch screen for the voter to make choices and record his/her votes.

“Global Election Management System (GEMS)”

The backbone of the election system that provides the functionality for ballot definition and layout, the downloading and uploading of memory cards and the tabulation and reporting of votes. Also known as GEMS.

“Header” Text information that appears on the ballot identifying the race title, question and issue description, as well as the number of selections available to the voter for the race.

“Hide Ballot”

The visually impaired ballot station option to hide the visual portion of the ballot as the audio ballot is played. This option is programmed to the voter smart card.

“High Contrast”

Ability to change the AccuVote-TSX presentation to black and white for low vision voters.

“Host Computer” The GEMS computer, interfacing with GEMS clients and voting devices.

“Host Name” The name or IP address of the GEMS host computer.

“Key Card”

The ‘Key Card’, created using the Key Card Tool that can be used to encode the security key values on the election’s smart card reading equipment.

“Key Card Tool”

The Key Card Tool, a stand-alone application, that allows the user to create a smart card encoded with user-defined security codes or *keys*, and is also used to encode supervisor and administrator type smart cards with the election’s security key. The Key Card Tool is also used to update the card’s supervisor and administrator password.

“Keypad”

A telephone-style keypad used to enter commands in the audio ballot on the AccuVote-TSX.

“Language”

A ballot display selection available on the AccuVote-TSX, which allows the voter to select a ballot in the language of their choice, (e.g. English, Spanish, Chinese, Japanese, Vietnamese, Tagalog, Korean, and French). These are languages that have been used on the AccuVote-TSX. Languages are defined in the GEMS ballot layout software application.

“Large Text”

The ability to increase the size of ballot text for the benefit of visually impaired voters on the AccuVote-TSX.

“Last Oval or First Oval Deck”

A test deck used in an optical scan election. This consists of a single ballot card per precinct with either the first candidate or the last candidate in a race marked for each race. This deck or card is specific to a precinct and is run thru the corresponding precinct memory card. The purpose of this test is to check that the precinct IDs and ovals on the ballot match the expected data format of the precinct memory card for the precinct optical scanner or central count optical scanner. This test is used to populate a count into each precinct to ensure database version control has been maintained, that all precincts and memory cards match the GEMS database, and that data is accurately flowing between the precinct or central count scanners and the GEMS host system. This test and test deck are not sufficient as a total test and shall be used in conjunction with the Logic and Accuracy test decks (LA5, LAN, or LAmx).

“Logic and Accuracy Deck (5 or n or max)”

A test deck comprised of optical scan ballots that is used to test the logic of a precinct memory device in the AccuVote-OS or an absentee precinct using an AccuVote-OS device in central count mode. This deck can be ordered to give a 1,2,3,4,5 pattern to candidates in a race. For example, if there are seven candidates and a write-in – eight ovals in the race – an LA5 deck would give a 1,2,3,4,5,1,2,3 pattern. This deck can be ordered with any N number of the pattern. This deck can also be ordered as an “LA max” deck. In this case, the largest number of candidates on the ballot will define the “maximum” number of the pattern. If there are 15 candidates, then the deck would consist of 1 ballot for the 1st candidate, 2 ballots for the 2nd candidate, etc., up to the 15th candidate, which would have 15 ballots voted for the last candidate. This deck would have a total of 120 ballots. As the county determines that decks are getting too large, they may use an LA5 deck to simply assign a 1,2,3,4,5,1,2,3,4,5,1,2,3,4,5 pattern to large candidate races.

“Machine ID” An AccuVote-TSX unit is given software tracking number or “Machine ID” during the initial start-up of the AccuVote-TSX in order to track election results by Machine ID at a polling location. This is not the same as the unit serial number.

“Memory Card” A solid state memory device utilizing industry standards for data storage of election and ballot information. It is a removable electronic media containing the election definition for both the AccuVote-OS and AccuVote-TSX. The memory card is also used to accumulate and tally election results. Also known as PCMCIA card or “PC Card.”

“Multi-Vote Deck”

This test deck is produced by a print vendor’s automated test deck process. Where a county is using a certified printer to print the AccuVote optical scan ballots, the county will need to prepare its own test decks to test for “vote for more than one” races to confirm that it is programmed for more than one candidate. This deck is produced for Ballot Styles where multiple votes (Vote For Two or more) are authorized. All races that are “Vote for one” are ignored in this deck. The first ballot is the “overvote” ballot. Each race has one more prefilled oval than allowed for the race. The next set of ballots rotate in combinations of the number of votes allowed, e.g. with Vote for Three and 6 candidates, the deck would produce a ballot for ovals 1,2,3 followed by 2,3,4, then 3,4,5, and then 4,5,6; continuing on to the last oval in the race. Tabulation would be 1 vote for first and last candidate, 2 votes for 2nd and 2nd from last, 3 votes to the 3rd and 3rd from last and so on until the candidates in the middle are receiving the maximum number of votes allowed.

“Number to Vote For” The number of candidates, responses or parties that a voter may select in a race without incurring an overvote.

“One Click Vote” The ability to make an alternative selection on the ballot on the AccuVote-TSX without having to click twice in order to disable an existing selection.

“Official Election Mode”

Official Election Mode is the operating mode in which the official election occurs. This application mode differs from “test mode”, where all administrative functions take place such as machine settings, testing, and diagnostics.

“Overvote”

The condition of voting for more candidates or selections than a race allows. The AccuVote-TSX does not allow a voter to vote for more than the “Vote For” limit of selections. The AccuVote-OS can be programmed to prevent an overvote.

“Party”

The political party affiliation of candidates for federal, state and central committee offices.

“Password”

An authentication of the user’s access to the GEMS, AccuVote-OS, or AccuVote-TSX device.

“PC Card”

Known as PCMCIA card or memory card. Also see “Memory Card”

“PCMCIA Card”

Known as “PC Card” or “Memory Card”. Also see “Memory Card”

“Phone”

The telephone number used for modem transmission.

“Poll Worker Card”

A special smart card programmed with the ability to put the AccuVote-TSX into voter card creation mode or

to close the polls and generate totals reports. Also known as “Supervisor Card.”

“Power”

The Power status indicator; defined as either charging (yellow bar on screen) or AC off line which means the AccuVote-TSX is operating off the battery. The AC offline indicator is a red bar that shows the remaining percentage of battery charge available. The AccuVote-OS also indicates when the AC is offline.

“Precinct” The smallest division of the electorate within a county, city, or district identified by geographic boundaries defined by the local election official. The precinct is expressed either as a base precinct, a geographical unit in which voters vote, or a report precinct, to which election results are reported.

“Programming Election Media”

The act of transferring election and ballot information to election media.

“Protocol” A set of parameters governing the communication and transfer of information between the host computer and the AccuVote-TSX unit.

“Protection of Results Data”

All results data is protected using standard data encryption methods and by system design functionality. The encryption process makes information indecipherable to protect it from unauthorized viewing, tampering or use.

“Protective Counter”

The total count of all ballots cast on the AccuVote-TSX since the manufacture of the AccuVote-TSX unit. Also known as “System Counter.”

“Provisional Voter Ballot”

Pursuant to Elections Code section 14310, a ballot given to a voter claiming to be properly registered, but whose qualification or entitlement to vote cannot be immediately established upon examination of the index of registration for the precinct or upon examination of the records on file with the county elections official, which includes the list of absent voters.

“Public Counter”

The total number of ballots cast on an AccuVote-TSX during a specific election. Also known as the Election Counter.

“Removable Storage Media” The external media which stores the election, audit and / or ballot information programmed for the AccuVote-OS and the AccuVote-TSX, and to which election results are tallied once ballots are counted. Also referred to as the Memory Card, PCMCIA card or PC card.

“Recount” The configuration of an election for recounting one or more races, involving programming selected memory cards and uploading and reporting results for a recount reporting set.

“Report Precinct” The results of ballots counted in base precincts are tallied to report precincts.

“Rotation”

The candidate rotation rule determines the order candidates are to appear on ballots in a particular geographic area.

“Running State”

In the running, or “Set for Election” state, no modifications are allowed to the election definition. In this state, the removable media is prepared for distribution to the AccuVote-OS and AccuVote-TSX.

“Semi-Official Canvass”

The process of collecting, processing, and tallying ballots and, for statewide elections, reporting results to the Secretary of State on election night. The semi-official canvass may include some or all of the absentee vote totals. The semi-official canvass is contrasted with the official canvass which begins not later than the first Thursday following the election, and for statewide elections shall result in final certification 28 days following the election (Elections Code section 15372)

“Serial Number” The AccuVote-OS serial number can be located on the back of the unit. The AccuVote-TSX serial number can be found on a label on the external surface of the AccuVote-TSX. This is different from the Machine ID, which is used by the software application.

“Scale %” The scaling value applied to the AccuVote-TSX image; programmed in GEMS.

“Scale” The increasing or decreasing of an image from nominal size.

“Straight Party”

A party selected in a straight party or endorsement race which automatically counts candidates endorsed by the party in all straight party-voted races, subject to the straight party tally rule defined for the election. *Straight party voting is not allowed in California.*

“Supervisor Card”

A special smart card programmed with the ability to put the AccuVote-TSX into voter card creation mode or to close the polls and generate totals reports. Also known as “Poll Worker Card”.

“System Total” The number of ballots cast on the AccuVote-TSX unit since the date of the manufacture of the AccuVote-TSX. It is also referred to as the “Protective Counter”.

“Set-up Diagnostics”

A system test of the software and hardware of the AccuVote-OS and AccuVote-TSX prior to entering ballot logic.

“Smart Card Authentication”

The process by which a Smart Card is inserted into the AccuVote-TSX and parameters verified for the functions being requested. These range from access security to election security to administrative security functions.

“Source Code”

The version of a computer program in which the programmer’s original programming statements are expressed in a source language, which must be compiled, assembled and linked into equivalent machine executable object code, thereby resulting in an executable software program.

“TS Text” Sets of files residing in GEMS, containing multi-language operational instructions which are programmed to the AccuVote-TSX.

“Type or Network Type”

Type refers to the type of network connection used for transmission; for example, ‘Local Area Network’ if the computer is networked to a hub.

“Undervoted Race”

A contest in which the voter selects fewer choices than the maximum number of choices on that contest.

“Unit”

The designated machine number in the Vote Center.

“Upload”

The process of transferring election results from the AccuVote-OS and the AccuVote-TSX units to the GEMS host computer.

“User Name”

The network user ID.

“Version”

The vote center/machine ID download version.

“Visually Impaired Ballot Station (VIBS)”

Visually Impaired Ballot Station (VIBS), an AccuVote-TSX plug-in feature that allows ballots to be voted and cast in audio format.

“Visual Ballot”

The ballot displayed on the touch screen, either when voting a non-VIBS ballot, or when voting a VIBS ballot without the ballot display hidden.

“Vote Center”

A physical polling location, containing one or more voting devices.

“Voted Ballot”

A ballot which has been marked by the voter.

“Votes Cast”

The number of votes cast in a tally, distinct from the number of ballots cast.

“Voting Device”

A Premier ballot counting device; either an AccuVote-OS or AccuVote-TSX.

“Voting Mark” The mark on a ballot created by the voter’s selection of preferred candidate or measures.

“Voter Access Card”

This card indicates the appropriate ballot to present to the voter and permits an eligible voter to cast a ballot on the AccuVote-TSX. The card will not allow multiple voting or any access to the election management system. Also referred to as a voter “Smart Card”.

“Voter Exit Screen”

The Voter Exit Screen prompts the voter to remove the card from the card reader. When the card is removed, the system returns to the Open Polling Place State.

“Voter Instruction Screen”

The Voter Instruction screen presents the voter with a simple set of instructions for making voter selections and recording the ballot. It appears after the voter inserts the access card.

“Write-In” Upon choosing the write-in option on the AccuVote-TSX, which allows a voter to select a person whose name does not appear on the ballot, the voter is presented a screen that allows him/her to spell out the name of their candidate by touching the appropriate letters. When the voter touches the Record Write-In button, the name written in appears on the screen showing the applicable contest. The name written in will also appear on the Summary Screen and the AVPM.

The voter can write-in a name on the AccuVote-OS ballot. The voter must fill in the

oval next to the write-in name for the vote to count, pending whether the write-in name is a qualified write-in candidate.

Additional definitions may be found in the various User and reference guides that are listed in the appendix

2. Ballot Definition

2.1. Overview

The GEMS ballot layout software is a fully integrated software package. This integrated software is a single program of code that provides for importing of sub-precinct and consolidated precinct information as well as race, candidate and question information from the Election Management system. Information may be entered manually as well. It then is able to lay out the ballot using a fully Windows compliant graphical user interface.

The GEMS system generates the ballots automatically taking the user defined specifics, ie., rotation, font size, ballot definitions and applying them with the touch of a button. Ballots may then be viewed on screen and changed as needed. The many Administrative reports available offer the tools needed for proofing and may be viewed on screen or printed.

2.2. Paper and Printing Specifications

Ballots printed for the Premier system must conform to unique specifications. These specifications are outlined and in detail in the Premier Ballot Specifications Revision document and as such will be referenced here. They include specifications for paper weight, color, ink and many other items. California EC 13002 specifies that ballots shall be tinted and watermarked or overprinted with a design, to be furnished by the Secretary of State, so that the watermark or overprint shall be plainly discernible.

2.3. Layout Requirements and Specifications

Detailed layout for ballots may be found in the GEMS Election Administrator's Guide. *Managing Ballot Artwork* in the *GEMS 1.18 User's Guide* includes procedures detailing the creation of ballot artwork in GEMS. *Managing Ballot Artwork* in the *GEMS 1.18 Reference Guide* describes the concepts behind the creation of ballot artwork in GEMS.

California EC Div 13, Chapter 3 (13200-13289) contains specific legal requirements for ballots.

3. System Installation and configuration

3.1. Hardware Requirements and Specifications

The GEMS host computer is used to run the GEMS software, and is configured by Premier. The GEMS server may run Windows 2000 or Windows 2003. The below servers are an example of the servers used to host the GEMS software.

Server Dell PowerEdge 2900 (Tower) and Rack Mount Model 2950

- Dual Core Intel Xeon 5120 4MB Cache (29W18) [222-6451]
- 2GB 533MHz Single Ranked DIMM (2G4D5S) [311-5727]
- Windows Server 2003 R2 5CAL (WSR2S) [420-5796]
- PERC 5/I Integrated Controller (PERC5II) [341-3018]
- Integrated SAS/SATA RAID 5 (MSR5N) [341-2999]
- 73GB SAS 3.5-inch 10K (73A10) [341-3028]
- Tower Chassis Orientation (TOWER) [310-7489]
- Redundant Power Supply with Dual Cords (RPS) [310-7407]
- Tower Bezel (TBEZEL) [313-4363]
- Dual Embedded Broadcom NetXtreme II 5708 Gigabit NIC (OBNIC) [430-1764]
- Broadcom TCP/IP Offload Engine Not Enabled (NTOEKEY) [430-1765]
- Electronic Documentation and OpenManage CD Kit (EDOCS) [310-7402]
- 48X IDE CDRW DVDROM (CDRWDVD) [313-4313]
- 1.44MB Floppy Drive (FD) [341-3053]
- Keyboard, USB (USBK4) [310-8170]
- Two-button USB Mouse (USBMW) [310-8171]
- Dell 22-inch widescreen analog flat panel (E228WFP)
- Soundblaster Audigy 4 sound card

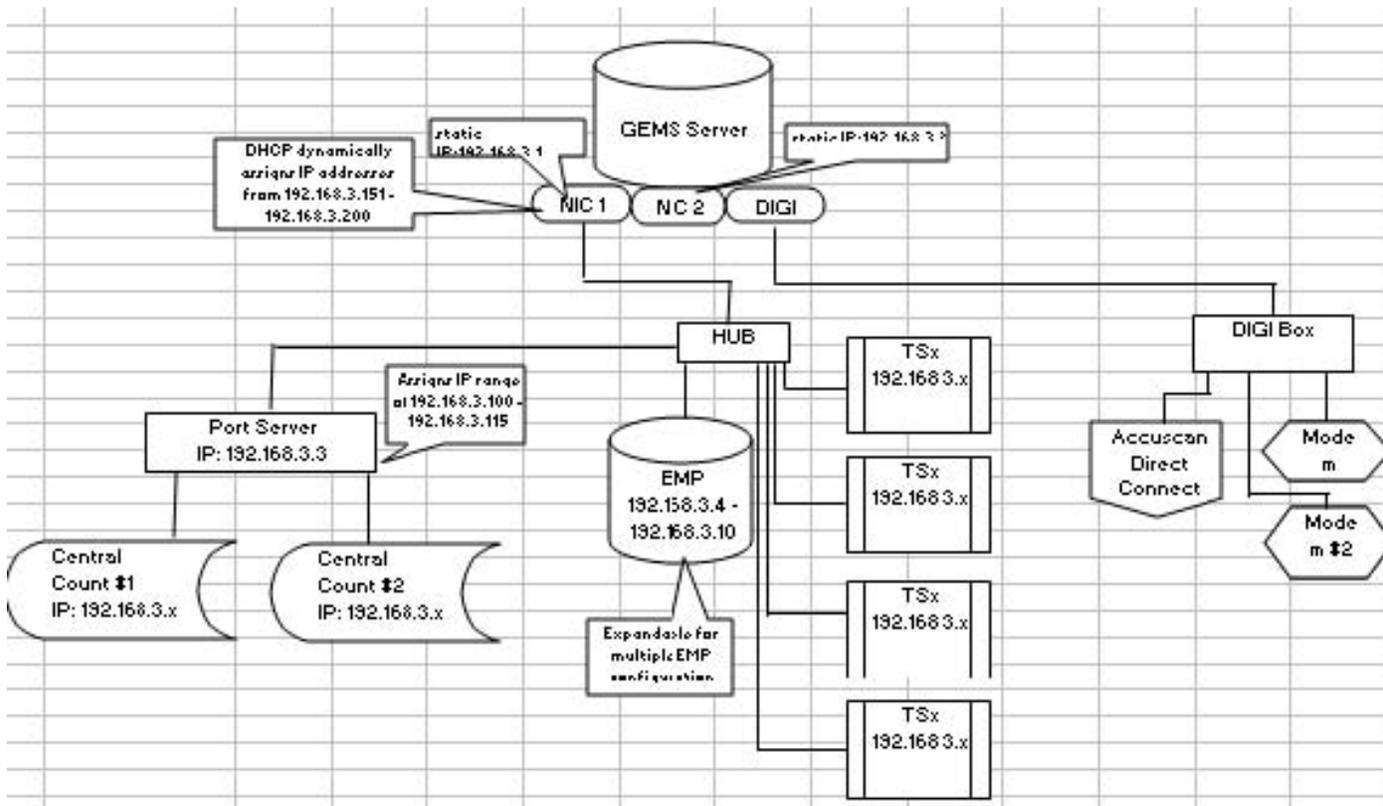
The VCProgrammer and Key Card tool may be run on a small Dell as described above or most often a laptop with a 9-pin serial com port that the smart card burner/reader may be connected.

The following external smart card reader devices may be used with the VCProgrammer and Key Card tool application:

- Securetech ACR-30S
- Securetech ST-100
- AMC Model 152

3.2. Hardware and Network Setup and Configuration

The system is a stand alone closed system, meaning it is not connected to the internet or outside networks. All tabulation peripherals operate independently and are stand alone. The transfer of data is accomplished through closed Local Area Network (LAN) connections and direct connections to the GEMS server. Proper network configuration is essential to efficient and accurate operation and is detailed in each hardware guide. A sample diagram is below and may change according to the actual configuration.



ry to configure a Premier GEMS Server are described in the document Windows Configuration Guide and shall be implemented.

The configuration requirements as supplied by Premier are as follows. Additionally, the Windows Configuration Guide provides additional information on configuring and hardening the GEMS server to prevent malicious attack or tampering. There may be other requirements as needed:

- 1 All network services and network ports are to be turned off, except those explicitly required to run the GEMS software;
- 2 the "autorun" feature in Windows is to be disabled;
- 3 the boot order is to boot from the hard drive only;
- 4 the BIOS is to be password protected to prevent changes to the boot order.

3.3 Software and Firmware Upgrades

Software upgrades shall be issued to each jurisdiction as directed by the Secretary of State. Firmware upgrades for the AccuVote-OS and AccuVote-TSX may be distributed by the State of California with the written permission of Premier. Installation of these components shall be the responsibility of the jurisdiction, which may or may not request assistance from Premier. Detailed installation instructions and testing are included with each products' user guide. Diagnostic and accuracy testing should be done after any software and / or firmware upgrade.

Operating system patches and upgrades should be downloaded from a separate computer, copied on a CD and also verified with Premier prior to installation.

3.4 Acceptance Testing

Acceptance testing is vital to any system, whether it is a new system or an existing system that has been modified. The procedures for each component of the system have been developed and are included in summary here and in detail in each component hardware guide. Acceptance testing applies to the initial testing period conducted following the initial delivery of election equipment to the jurisdiction from Premier.

See the system verification in the GEMS Election Administrators guide.

Verify that all of the expected functionality of the GEMS workstation is available. Mark each function on a signoff sheet once it has been verified. The following functions are to be verified:

1. Copy from CD
2. Restore database
3. GEMS version
4. Reports version
5. View card in Card Editor
6. Print ballot artwork
7. Print administrative reports
8. Record/play back audio
9. Download memory card
10. Upload memory card
11. Print results report
12. Perform a backup
13. Review GEMS User's Guide
14. Verify GEMS Read Me file
15. JResult Client version

AccuVote OS Diagnostic (Accuracy) Tests

Prior to use in either the central counting mode or precinct counting mode, hardware diagnostic and accuracy tests shall be performed on every AccuVote-OS to be used in the election. The following diagnostic and accuracy tests should be performed prior to any election. See the AccuVote-OS Precinct count Users Guide for more information.

To test the various internal components of the AccuVote-OS, go to the diagnostic mode on the AccuVote OS and perform the following:

- a. Verify the operation and setting of the Ballot Box deflector
- b. Verify the setting of the System date and time (consider seasonal time changes)
- c. Test the LCD monitor
- d. Test the System Memory of the AccuVote
- e. Test the operation of internal printer and ribbon
- f. Test the Serial Port on the back of the AccuVote
- g. Test all the scan sensors of the Ballot Reader
- h. Test the memory cards to be used in the election

Diagnostic and accuracy testing consists of those processes and procedures necessary to ensure hardware to be used in the election is working properly. If malfunctions are

encountered, corrections shall be made and recovery procedures implemented. Prior to use, verify and check all cabling and connections for each hardware component are properly attached and connected.

In the event any AccuVote-OS fails after official ballot processing has begun, diagnostic and accuracy tests must be successfully run on the (failed) component after it has been repaired, replaced, or adjusted (in a manner deemed sufficient by the responsible Election Official and / or designee) to require re-testing for accuracy) before the component is returned to service.

AccuVote-TSX Hardware Diagnostics

Each AccuVote-TSX to be used in an election or as a backup or spare device, needs to pass a standard diagnostic and accuracy test before placing a removable PCMCIA card in the voting machine for verification and testing. This allows the jurisdiction's technician to test and or work on the AccuVote-TSX well in advance of having election specific data and the preparation of the removable election media. By conducting diagnostic and accuracy tests in advance, any hardware and software error condition found can be promptly corrected prior to the election logic and accuracy testing cycle. See the AccuVote-TSX Hardware Guide and Ballot Station User's Guide for more detail and information on the diagnostic and accuracy testing of the AccuVote-TSX.

Diagnostic and accuracy testing of the AccuVote-TSX will include verification that all AccuVote-TSX hardware and software components are operational. These components include the audio, serial connectors, date and time, network connection, display, and the printer are functioning in its intended manner.

A historical log of hardware testing and error conditions should be kept by the jurisdiction for all components.

4. Election Setup and Definition

Introduction

This section discusses the recommended procedures for programming, proofing, testing, transmitting and reporting election results using the Premier voting system. This section breaks down those areas by the GEMS system, and the AccuVote-OS and AccuVote-TSX systems.

4.1 Global Election Management System (GEMS)

4.1.1 Programming of election management system / software

In California, the following setup is unique in California and should be set up in the GEMS database:

- Disable Bar Code – Under the “AccuVote-TS Option” in GEMS, do not select “Print Bar Codes”;
- Reject Overvoted Races and All Races Blank Voted – Under the “AccuVote-OS Options, Reject Settings” Tab, select the “Overvoted Races” and “All Races Blank Voted” under “Return Ballots With”;
- Using Report 195/196US and Version 1.96 – Under the “AccuVote-OS Options, AccuVote-OS Settings” Tab, select the “195/196US” under “Reports” and select “1.96” under “Version”;
- Do not use characters (e.g., “ % &”) in a label, vote center, race or candidate name.

4.1.2 General GEMS Programming Options

Election configuration options are defined under Setup in the GEMS menu bar. Setup options include general administration, users, regions, languages, voter groups, counter groups, ballot and race options, AccuVote-OS and AccuVote-TSX options, reporting sets, monitor scripts and finally, the printer audit function. Refer to Chapter 3 Election Setup in the GEMS User Guide for a more detailed explanation and instructions.

4.1.3 GEMS System (Logic) Proofing

GEMS System (logic) proofing involves verification that the election definition for the specified election is correct, the ballot layout is correct, the hardware is correctly configured and that it correctly tabulates and reports. There should be a checklist to verify all of the proofing steps have been conducted and completed.

System (logic) proofing is the in-house review of all election data and the interrelationships of that data. System (logic) proofing shall include, but is not limited to, verification of the correctness of the following:

- Assignment of jurisdictions participating in the election (districts);
- Linkage of precincts to offices in which the election will be held (precincts);
- Ballot content of each ballot type, including offices, district designations, candidate assignment and rotation, and ballot measures, all in the proper sequence (races and candidates);
- Preparation of instructions, candidates’ names, political designations, number to be elected, candidate rotation;
- Verification that all voting precincts have been correctly assigned to a polling location or mail ballot precinct;
- Formatting of headers and footers for each issue and electronic ballot page;
- Printing ballots to verify correctness of content;
- Hardcopy reports produced by the GEMS administrative reporting system should be printed to ensure desired formatting as well as verifying that expected results from testing were transmitted to the GEMS system;
- Ballot facsimiles produced by GEMS;
- Recorded audio files that may be presented to the voter;

Testing of hardware in the election configuration to verify correct tabulation of paper and electronic ballots;

4.1.4 – GEMS Data Transmission

Transmission to GEMS client devices is managed from the AVServer, Central Count Server, and Regional Server function consoles. All transmissions to and from the AccuVote-TSX, Election Media Processor, AccuVote-OS Precinct Count, and Central Tally System (CTS) are managed from the AVServer function console, while the AccuVote-OS Central Count is managed from the Central Count Server console. These consoles are modal, implying that they may remain active while other GEMS functions may be activated, such as the election results reports windows or the Results Server console.

4.2 AccuVote-OS Testing

Testing of election logic involves both data testing, ensuring the accuracy of cast ballots, and the system testing to ensure that data logic is consistent as it is transmitted from one component of the system to another - as it is downloaded onto memory cards, as ballots are cast, and as results are uploaded to the GEMS host computer application.

Logic and accuracy testing should be conducted on the tabulation memory devices to be used in the election. Diagnostic and accuracy testing is accomplished on the AccuVote-OS hardware to be used in the election. The diagnostic and logic and accuracy testing may be accomplished independently of each other, as one tests the memory device and the other tests the hardware. The County may choose to do logic and accuracy testing of the memory device and testing of the hardware to be used in the precinct together. However, the hardware and memory devices to be used in the election should be tested as described below.

These procedures could also be used during the post-election logic and accuracy testing process.

4.2.1 AccuVote-OS Diagnostic (Accuracy) Testing

AccuVote-OS diagnostic and accuracy testing should be performed on the AccuVote-OS units prior to each election to test and verify the hardware specifications of the AccuVote-OS unit are functioning in the correct manner.

The AccuVote-OS diagnostic and accuracy testing is testing the hardware functionality of the AccuVote-OS to verify the unit is operating in the intended manner. This testing includes using various checklists and directions. These items are included in the specific hardware user guides and a detail of the testing is outlined in the GEMS Election Administrator's guide in Chapter 4-Managing the election. These are also available through Premier's representatives

Any equipment, or component, that fails or malfunctions during maintenance and testing shall be serviced, repaired, or replaced and appropriately tested prior to the use of that equipment or component in any election. All equipment and specialized vote tabulating equipment must be certified for use in elections by the Secretary of State prior to use in any election.

Additionally, all equipment to be used in each election should be maintained at all times in good working order and all appropriate maintenance and other applicable logs should be kept for each piece of the system.

For each election, the responsible county elections official should prepare a list, including quantities, of all equipment to be used to tabulate votes during the semi-official and official canvass.

The AccuVote-OS units to be used in an election will have diagnostic and accuracy tests run. These tests include the following:

- Verifying or setting the AccuVote-OS System Clock for the Election Day time (anticipate any time changes that may occur prior to the date of the election);
 - Testing the LCD display;
 - Testing the AccuVote-OS System Memory;
 - Testing the memory cards to be used in the election;
 - Testing and verifying that the printer is working. (This operation prints a test pattern on the tape. This could be saved and attached to an AccuVote unit test sheet, along with other test reports, and saved as part of the election audit trail);
 - If the AccuVote-OS is to be used to upload or download memory card data, the serial port should be tested either via a diagnostic and accuracy test with a serial loop back connector, or by testing the upload or download function of the unit with the GEMS host computer system. Those AccuVote-OS units that are not used for uploading or downloading of data are not required to have the serial connection tested;
 - Testing the ballot box “deflector” (the mechanism that sorts ballots in the ballot box);
- Testing the AccuVote-OS, prior to the logic test, by using “diagnostic ballots”. These ballots test all read heads on the AccuVote unit and prints a detailed report verifying that all read heads are functional. This test is run on the AccuVote-OS units to be used in the election. The test print out should be attached to the AccuVote unit test sheet, These sheets are kept as part of the testing audit trail and have the date, time, serial number of the AccuVote-OS which produced the tape, and the initials of the person that ran the test.

Once diagnostic and accuracy testing has been completed on the AccuVote-OS units to be used in the election, the reports indicated above should be attached to an AccuVote-OS testing sheet which shows the serial number of the unit tested. Once diagnostic and accuracy testing is complete, a test should be done to verify that the associated memory cards is consistent with the election setup and proofing that has been accomplished for the election.

4.2.2 AccuVote-OS Logic and Accuracy Testing (L&A) Procedures

The logic and accuracy testing consists of those processes and procedures necessary to ensure that the vote tally programs and hardware correctly interpret, summarize and report voters’ marks for a specific election. This consists of a series of tests using test ballots which are made from actual printed ballots, or pre-determined test scripts. The results of those tests can be transferred to the GEMS system by transferring results from the memory cards via an AccuVote-OS to GEMS, and from the AccuVote-OS Central Count readers to GEMS.

Successful testing will demonstrate that each candidate and ballot measure receives the proper number of votes. The system reports the proper number of over and under votes, accepts only the proper ballot types and rejects improper ones; and the inactive voting positions are not being tabulated.

The Logic and Accuracy tests, conducted at the time of certification (or recertification) if necessary to the Secretary of State, storage logs or records, if any, and balancing reports, if any, shall be retained with material for that election for as long as the ballots are required to be kept for the election. (EC §15001 (2005))

4.2.3 AccuVote-OS Logic and Accuracy Testing

Logic and accuracy testing is conducted on the AccuVote-OS and AccuVote-OS Central Count. This testing method ensures the logic of the ballot programming is correct, and the testing reflects the accuracy of the votes cast for each individual oval position tested.

To conduct a logic and accuracy test, logic and accuracy test ballots should be prepared, at a minimum, for each ballot type in the election. These regular official ballots shall be marked “TEST” or otherwise clearly identified as test ballots.

The logic and accuracy test deck is generally made up of “First Oval or Last Oval” ballots for each precinct, LA5, LAN, or LAmx ballot decks, and, if the election has a race where the voter can vote

for more than one candidate, multi-vote ballots. The following description of the test decks are recommended procedures should a jurisdiction choose to use the test deck.

- **First Oval / Last Oval** - Test ballots consist of one ballot from every precinct in the election with the first or last oval filled. If the “last” position is a write-in, the deck will have the last position candidate marked in every contest. These will be processed as part of the accuracy test explained in these use procedures. Once the card is run, a result tape can be printed. This tape is kept as part of the election audit. The serial number on which the test was run will be written on the tape, as well as the initials of the person that ran the tape and verified that the first or last candidate correctly received the votes. Finally, the memory cards can be uploaded so that results are verified and confirmed on GEMS. A verification on GEMS can be made to ensure that this test creates 100% precincts counted report.

LA5, or LAn, or LAmx Test Deck -A county may choose to make their own test decks from “blank” ballots ordered from their printer. If a 3rd party printer has been used, this process may be required. Therefore the test deck must reflect a test that checks each candidate position with a known number of votes for each candidate. If the County has a print vendor print the ballots, an automated deck consisting of an LA5, or a specific specified pattern (LAn), or an LAmx deck can be ordered. This deck is made up of election specific ballots that have been marked with a predetermined pattern of votes. For example, an LA5 deck will provide a race with a 1,2,3,4,5 pattern of votes that will be cast for candidates in every contest. For example, the 1st candidate will receive one vote, the 2nd candidate will receive 2 votes, and the 3rd candidate will receive 3 votes and so on until all candidates have had votes cast for them. If there are more than 5 candidates in a contest, the pattern will repeat so that the 6th candidate will receive 1 vote, the 7th candidate will receive 2 votes and so on until votes have been cast for all candidates.

If there are fewer than 5 candidates, the pattern will only go up to the highest number of candidates in that race. At a minimum, this deck is created for at least one precinct in each ballot style, or as determined by the Election Official. When an LA5, “n”, or max test ballot deck is run for each ballot style, a “first or last” oval deck should also be run for all remaining precincts to verify that all precincts are tested for proper printing of precinct ID marks on each ballot and that the appropriate “precincts counted” numbers are achieved.

The purpose of any of these L&A decks is to test that all candidates and races on all ballot styles are counting correctly. After each L&A deck is processed thru the AccuVote-OS unit in precinct or central count mode, a precinct report can be generated to verify that the correct votes are being tabulated by the AccuVote-OS unit and/or by GEMS in the case of central count AV or mail precincts.

It is recommended that as many L&A decks be used as is reasonable for the election, given the time and resources available. However, at a minimum, the L&A deck must be run for every ballot style. For example, an even year primary may preclude a county from running an LA5 (or other L&A) deck for every precinct due to the number of ballot styles and parties in an election.

For primary elections, an L&A deck should be created for each of the parties in a ballot style.

When using the automated L&A test decks, it may be noted that for offices that rotate across districts, an Election Summary Report on GEMS may not maintain the 1,2,3,4,5, etc. pattern. In this case a report should be printed so that individual precincts may be viewed with results isolated for each candidate and race, thereby clearly showing the expected pattern of votes within each race.

- **Multi-vote test deck:** This test deck is produced by a print vendor's automated test deck process. Where a county is using a certified printer to print the AccuVote optical scan ballots, the county will need to prepare its own test decks to test for "vote for more than one" races to confirm that it is programmed for more than one candidate. This deck is produced for Ballot Styles where multiple votes (Vote For Two or more) are authorized. All races that are "Vote for one" are ignored in this deck. The first ballot is the "overvote" ballot. Each race has one more prefilled oval than allowed for the race. The next set of ballots rotate in combinations of the number of votes allowed, e.g. with Vote for Three and 6 candidates, the deck would produce a ballot for ovals 1,2,3 followed by 2,3,4, then 3,4,5, and then 4,5,6; continuing on to the last oval in the race. Tabulation would be 1 vote for first and last candidate, 2 votes for 2nd and 2nd from last, 3 votes to the 3rd and 3rd from last and so on until the candidates in the middle are receiving the maximum number of votes allowed.

A logic and accuracy test should be performed on the AccuVote-OS units and the Central Count readers as applicable. A precinct results tape should be printed for each logic test on the AccuVote-OS units. This tape should show the expected pattern of votes for each candidate race based on the test deck created by the County, or ordered from the ballot printer. As the AccuVote-OS units is tested, it should be verified for the expected results, uploaded to GEMS, and reports printed that are confirmed to have identical results to the precinct results tapes printed during the test. A recommended process for conducting a logic and accuracy test on the AccuVote-OS unit follows:

- Run an LA5 (n, or max) deck for every style that will be used for the central count and/or AccuVote-OS precinct count ;
- Run a First Oval / Last Oval deck for all precinct not included in the LA5 (n, or max) decks;
- Print the reports for the AccuVote-OS and examine for expected results pattern;
- Upload the memory cards to the GEMS system;
- Once the memory cards have been loaded with test data, the memory cards should be uploaded to the GEMS host. After all memory cards have been uploaded, a GEMS Summary Report, a specific precinct report or a Statement of Votes Cast (SOVC) should be printed and used to compare the results received by GEMS with the precinct tapes printed during the L&A test deck or "first or last" oval deck runs of the AccuVote-OS unit.

4.3 AccuVote-TSX Testing

Testing of election logic involves both data testing -ensuring accuracy of cast ballots, and system testing to ensure that data logic is consistent as it is transmitted from one component of the system to another - as it is downloaded onto memory cards, as ballots are cast, and as results are uploaded to the GEMS host computer application.

These procedures could also be used during the post-election logic and accuracy testing process.

4.3.1 AccuVote-TSX Diagnostic (Accuracy) Testing AccuVote-TSX diagnostic and accuracy testing should be performed on the AccuVote-TSX units prior to each election to test and verify the hardware and software specifications of the AccuVote-TSX unit are functioning in the correct manner.

The AccuVote-TSX diagnostic and accuracy testing is testing the hardware and software functionality of the AccuVote-TSX to verify the unit is operating in the intended manner. This testing includes using various checklists and directions. These items are included in the specific hardware user guides as well as through Premier's representatives.

Any equipment, or component, that fails or malfunctions during maintenance and testing shall be serviced, repaired, or replaced and appropriately tested prior to the use of that equipment or component in any election. All equipment and specialized vote tabulating equipment must be certified for use in elections by the Secretary of State prior to use in any election.

Additionally, all equipment to be used in each election should be maintained at all times in good working order and all appropriate maintenance and other applicable logs should be kept for each piece of the system.

For each election, the responsible county elections official should prepare a list, including quantities, of all equipment to be used to tabulate votes during the semi-official and official canvass.

Testing for the AccuVote-TSX units to be used in an election include the following:

- Verifying or setting the AccuVote-TSX System Clock for the Election Day time (anticipate any time changes that may occur prior to the date of the election);
- Testing the AccuVote-TSX Card Reader;
- Testing the AccuVote-TSX Serial Port;
- Testing the AccuVote-TSX Audio;
- Testing and verifying the touch screen is accurately recording a selection on the screen;
- Testing the memory cards to be used in the election;
- Testing and verifying that the printer is working.

Any hardware failure of a component during testing will necessitate re-testing of that hardware with election specific data prior to placing that hardware back in use for the election.

Once diagnostic and accuracy testing has been completed on the AccuVote-TSX units to be used in the election, the AccuVote-TSX testing sheet should be recorded and signed by the authorized county tester and stored. Following the diagnostic and accuracy test, a logic and accuracy test should be done to verify that the logic and accuracy on the AccuVote-TSX unit is consistent with the election setup and proofing that has been accomplished for the election.

4.3.2 AccuVote-TSX Logic and Accuracy Testing Procedures

The logic and accuracy testing consists of those processes and procedures necessary to ensure that the vote tally programs and hardware correctly interpret, summarize and report voters' marks for a specific election. This consists of a series of tests using test ballots or pre-determined test scripts. The

results of those tests can be transferred to the GEMS system by transferring results from the memory cards via an AccuVote-TSX to GEMS.

Successful testing will demonstrate that each candidate and ballot measure receives the proper number of votes. The system reports the proper number of over and under votes, accepts only the proper ballot types and rejects improper ones; and the inactive voting positions are not being tabulated.

The following are some recommended procedures for the logic and accuracy test for the AccuVote-TSX:

The logic and accuracy tests will be conducted using test materials in such a manner as to meet these guidelines. All tests shall result in reporting that matches predetermined results. All reports and test materials must be retained as part of the official election record for the time period dictated by law. [EC §15001(c)(1)];

The Logic and Accuracy tests, conducted at the time of certification (or re-certification) if necessary to the Secretary of State, storage logs or records, if any, and balancing reports, if any, shall be retained with the election material as long as the electronic ballots are required to be kept for the election. (EC §15001 (2005));

The responsible elections official or authorized designee shall prepare the logic and accuracy test ballot decks or scripts and make it available for testing. The results reports of the logic and accuracy tests must be available for inspection and sign off by the county elections official and / or the authorized designee;

The logic and accuracy testing for the AccuVote-TSX and the AVPM audit trail should include the following considerations to represent and simulate an election environment:

- Testers should vote to simulate actual election conditions;
- The election test script should have a random sample of precincts for the election. For a primary election, the parties, including the “crossover” parties, were applicable as well as each unique style should be included;
- The test script should test for write-ins, undervotes, blank votes and a number of blank ballots;
- The testing should include the printing of the AVPM audit trail to test the accuracy of the audit trail;
- The AVPM audit trail should be verified against the AccuVote-TSX results report and the GEMS results report.

The election administrator or authorized designee should enter the voted selections, and cast the votes in a predetermined voting pattern. The voting pattern should insure each candidate and each ballot measure receives at least one vote. The test should include at least one under vote (it is not possible to over vote on the AccuVote-TSX) and accepts only the proper ballot types.

The resulting logic and accuracy vote tallies shall be compared in detail with the

predetermined logic and accuracy vote tallies. Any differences between the two logic vote tallies needs to be resolved, and logic and accuracy testing shall be performed as many times as may be necessary to achieve a logic and accuracy vote tally identical to the predetermined logic vote tally.

If the results report shows any variance in the tabulation of votes, the cause for the error shall be ascertained and corrected and an errorless count shall be made before the system is approved for use in counting votes. Pre-conditions for performance of tests, including test decks.

4.3.3 AccuVote-TSX Logic and Accuracy Testing

The logic and accuracy test is an essential method of testing electronic ballots to be used in that particular election, ensuring that the AccuVote-TSX units perform properly. The purpose of this test is to ensure that the ballot used with a particular election will function properly when run with the ballot tabulation software for that election.

The tests may be conducted by using a combination of automated and manual tests that incorporate pre-determined test scripts to verify that the system is correctly and accurately recording, tabulating, and reporting vote results. These tests which may be conducted are:

- a. An automated test script which provides a unique vote value for all candidates within a race, and tests all ballot styles and rotations in the election. This data is uploaded to GEMS. The summary report from the AccuVote-TSX is then compared with the Summary Report of the GEMS server to ensure that tabulation and reporting of candidate votes in all races is occurring accurately on both systems. A report is used to verify that the results are identical at the precinct level.

This process tests the reporting functions of GEMS and the AccuVote-TSX as well as providing verification that the election logic is mapped correctly between the GEMS server and the AccuVote-TSX ballot styles in the precincts;

- b. An automated test process which gives votes to all candidates in all precincts. This test verifies that all precincts and races are correctly mapped between the GEMS database and the AccuVote-TSX ballot station;

- c. Use of one of two possible manual vote tests: A manual testing process, which incorporates a pre-determined random script of votes for all races and ballot styles as described below, or a manual testing process, aided by the testing software, which provides a manual vote for each candidate in each ballot style of the election, but provides a unique value to all candidates within a race. Votes will be checked in GEMS to determine the logic and accuracy;

- d. Another test following the manual or automated logic and accuracy test is to print the ballots on the AccuVote-Printer Module (AVPM) during this

process so that the AVPM testing occurs for races and ballot styles for that election. These printouts become part of the audit trail which shows that the AccuVote-TSX hardware and software are accurately recording and printing ballots as voted for all candidate and race combinations.

If a voting machine or the central tabulating system does not accurately count the test script or test vote, the cause for the error shall be ascertained and corrected. An errorless count shall be successfully produced before the system is approved for use in counting votes.

4.4 AccuVote-OS and AccuVote-TSX Audit Log Retention

The GEMS Audit log contains a complete record of all transactions that have occurred in the election in GEMS, ordered by date and time. These should be printed and retained as part of the official election. This log is located in the drop down list under the GEMS menu.

Specific transaction in the AccuVote-OS Precinct Count is recorded to the Audit Log, which is stored on the memory card. The Audit Log can neither be deleted or altered other than by means of the automatic posting of event transactions to the log. The audit log will be printed out at the end of Election Day and posted.

All system operations performed on the AccuVote-TSX unit are logged to the unit's System Log. All election related operations are logged to the Audit Log. When an installed memory card has been programmed with election data, system operations are logged to both the Audit Log and the System Log. The Audit Log is stored on the memory card and the unit, and the System Log is stored on the unit only.

As with the GEMS System logs, the hardware audit logs should be printed and retained as part of the official election. Please refer to the Ballot Station User Guide and the AccuVote-OS precinct count user guide for more detail.

4.5 Public Logic and Accuracy Board and Certification of Testing

The jurisdiction may appoint a Logic and Accuracy Board to oversee the public logic and accuracy testing. The public logic and accuracy board shall be appointed by the responsible election official or by the authorized designee. The Counties are responsible for the development of its Logic and Accuracy Board.

4.6 Ballot Tally Programs

A copy of the ballot tally program used for the election shall be sent to the Secretary of State prior to each statewide election in the timeframe prescribed by law [EC§15001(a) (2005)]. Any subsequent changes to the ballot programs must be resubmitted to the State.

Seven days before each statewide election, the elections official shall certify to the Secretary of State the results of the logic and accuracy tests as well as the accurate functioning of all ballot counting equipment. This certification shall also affirm the use of the same equipment for pre-election testing and for semi-official and official vote canvasses. In the event of a change to the ballot tally program occurring after this certification, an amended certificate shall be submitted no later than the day before the election. EC §15001(a) (2005)] In the event any of the host tabulation computer equipment is repaired, altered or replaced following the certification specified in the above section and prior to completion of the official canvass of the vote, an amended certification of logic and accuracy testing and a revised list of equipment used must be submitted to the Secretary of State not later than submission of official canvass results.

4.7 Election Observer Panel

All procedures prescribed in this procedures manual should be carried out in full view of the public insofar as feasible. In addition, the responsible elections official shall devise a plan, subject to the approval of the Voting Systems Panel, whereby all critical procedures of the vote tallying process described in this procedures manual are open to observation by an Election Observer Panel. Representatives of the qualified political parties and representatives of the news media shall be among those invited to serve on this Panel and shall be given the opportunity to observe that the correct procedures have been followed in the receiving, processing, and tallying of all the voted ballots. The Election Official shall appoint an Election Observer Panel; failure of any or all invited parties to participate on the Panel shall not stop procedures from continuing as otherwise required by law.

5. Polling Place Procedures

5.1 Precinct Supplies, Delivery and Inspection

Precinct Supplies

In addition to those supplies required for the conduct of elections generally, the precinct official should supply to each precinct a sufficient quantity of the following:

For AccuVote optical scan precincts

- a. Marking devices compatible with the AccuVote-OS Voting System as recommended by Premier.
- b. Ballots of such form as required for tallying by GEMS. Prior to delivery, ballots should be inspected to ensure the correct precinct.
- c. Secrecy envelopes or folders in sufficient quantity to conduct the election. These envelope/folders must entirely cover the ballot area on which voting marks are made and provide secrecy of voted ballots until the ballots are deposited in the ballot box.
- d. One or more ballot boxes or containers that may be sealed or locked, into which is placed each voter's ballot(s).
- e. Containers or envelopes in which to enclose the following: (1) election supplies; (2) voted ballots; (3) provisional, voted absentee, spoiled, unused and cancelled ballots. At the option of the Election Official, the container provided in Item d may be used for all or part of this requirement.
- f. Ballot Statement.
- g. Other forms, logs, and seals for containers, equipment and supplies necessary for the conduct of the election.

For AccuVote-TSX precincts

- a. AccuVote-TSX with AVPM including sealed canister and paper roll.
- b. Keys to open the PCMCIA door and printer compartment.
- c. Voter card encoders with backups.
- d. Voter access cards 3 if only one unit, 10 if more than one.
- e. AccuVote-TSX units may be used as backup Voter Card encoders.
- f. AVPM units, security canisters, seals and paper rolls (1 per AccuVote-TSX), if needed.
- g. Privacy screens.
- h. Demonstrator unit if available.

5.2 Polling Place Setup

For the AccuVote-OS

The precinct officer shall check that the following has been delivered and verified:

- a. An AccuVote-OS tabulator with the correct memory card installed. This can be verified by inspecting the printed Results Tape. If Multiple Precinct Processing is to be implemented, the AccuVote-OS device shall be located so that it is equally accessible to voters and precinct officers of each precinct.
- b. A ballot box compatible with the AccuVote-OS. It has three compartments or bins with slots. During operation, the AccuVote-OS is inserted into the top of this ballot box, and processed ballots emerging from the AccuVote-OS are fed into the right and center bins.
- c. Two keys appropriately labeled. One key will open the printer compartment on top of the AccuVote-OS. Another key will open all the doors of the ballot box.
- d. On receipt of the AccuVote-OS, verify that the identification number on the AccuVote-OS is the same number that is listed on the Voting Device Report or precinct supply list. The serial number is located on the back of the AccuVote-OS next to the plug.
- e. Check the number on the seal that locks the memory card slot in place. This is the same number that is listed on Voting Device Report or precinct supply list. Report any irregularity (broken seal, incorrect seal) to the Election Official. Voting may commence, but ballots are to be deposited in the left side auxiliary bin until corrective action, if any, is taken or directed by the Election Official.

AccuVote-OS Ballot Box set up

- a. Verify that no ballots remain in any of the ballot box bins from testing or previous elections. Invite any persons assembled at the polling place to view the empty ballot box and observe the closing of the ballot box;
- b. Remove the ballot slot cover on top of the ballot box;
- c. Lift the AccuVote-OS and slide it into place on the top of the ballot box, leaving enough room in the back of the unit to turn the power switch on. Thread the power cord through the chute in the ballot box and plug it into the back of the AccuVote-OS unit;
- d. Push the AccuVote-OS back against the ballot box plug. Lock the front door of the ballot box to firmly secure the AccuVote-OS to the ballot box;
- e. Close and lock all ballot box doors. The auxiliary bin door may be left open.

For the AccuVote-TSX

To set up the AccuVote-TSX with the AVPM refer to the AccuVote-TSX Poll workers Guide and complete the following steps:

- a. Assemble voting booths with AccuVote-TSX;
- b. Install AVPM, feed paper and load security canister. The poll workers will be given instructions on the assembling of the AVPM to the AccuVote-TSX;
- c. Plug the AccuVote-TSX into the AC outlet;
- d. Unlock side door, power the unit on, close the door and relock the side door;
- e. Verify that the serial number and precinct on the security canister and the display screen match with one another. Verify the chain-of-custody log is correct. If there is a discrepancy, contact the county help desk to report the discrepancy;

- f. Report any problems to the appropriate election official / jurisdiction hotline and / or help desk;
- g. Make a demonstrator device available, if applicable.

5.3 Opening the Polls For the AccuVote-TSX To open the polls with the AccuVote-TSX:

- a. Perform a printer test to verify the printer is working;
- b. Allow a zero report to print, and designate the authorized election officials to verify the zero counts in all races and sign in appropriate space on the tape;
- c. Start the take up spool on the AVPM to the canister where it will be stored;
- d. Lock the printer compartment;
- e. The AVTSX key must stay in control with the authorized poll worker at all times
- f. Before the precinct board allows votes to be cast on any machine, it shall proclaim aloud at the place of election that the polls are open.

For the AccuVote-OS For the AccuVote-OS Precincts:

To open the polls with the AccuVote optical scan precincts:

- a. Unlock the printer cover and turn the AccuVote-OS on;
- b. The AccuVote-OS will automatically print the Zero Tape report when it is turned "ON";
- c. Check the AccuVote-OS Liquid Crystal Display (LCD). The LCD indicates the poll number and the public counter are at 0. If the LCD display shows any number other than "0", turn off the unit and call the county help desk for further instruction;
- d. The Zero Tape is the final initialization report that shows no ballots have been counted. Depending on how the election memory card is programmed, it may also show zero vote totals for each race and measure
- e. If the Zero Tape does not automatically print when the AccuVote-OS is turned on, report the issue to the Election official. Voting may commence, but ballots are to be deposited in the left auxiliary bin until corrective action is taken;
- f. Verify that all candidate names and propositions displayed on the Results Tape are the same as they appear on the official ballot;
- g. Verify that all candidate names and propositions have a zero total;
- h. If any of the conditions described under "e" or "f" do not exist, this must be reported to the Election Official. Voting may commence, but ballots are to be deposited in the left auxiliary bin until corrective action is taken;
- i. The precinct board shall sign the zero tape. The zero tape is not detached. Invite any persons assembled at the polling place to view the zero tape. Roll or fold tape and lay the zero tape inside the AccuVote-OS. Replace and lock the printer cover. The AccuVote-OS is ready to accept ballots.

5.4 Polling Place

Procedures

The following are recommended polling place procedures for the AccuVote-OS and the AccuVote-TSX units:

For the AccuVote-OS

- a. Surrender of Absentee Voter Ballot: No person to whom an absent voter ballot was issued is permitted to vote at the polling place unless he or she surrenders the absentee ballot. The ballot is to be marked "SURRENDERED" and placed in the container marked for spoiled and unused ballots. The voter is then permitted to vote in the normal method for the precinct. If the voter cannot surrender the absentee ballot, that voter may be issued a provisional ballot.
- b. Voted Ballot Sealed: If a voter returns a voted absentee ballot, verify that the ballot is sealed and that the signature of the voter is on the identification envelope.
- c. During the day, at least every hour, inspect the AccuVote-OS to ensure that the power cord is connected and screen is displayed properly.
- d. Offer instructions to voters in the proper method of inserting a voted ballot into the AccuVote-OS.

For the AccuVote-TSX Precincts:

- a. Surrender of Absentee Voter Ballot: No person to whom an absent voter ballot was issued is permitted to vote at the polling place unless he or she surrenders the absentee ballot. The ballot is to be marked "SURRENDERED" and placed in the container marked for spoiled and unused ballots. The voter is then permitted to vote in the normal method for the precinct. If the voter cannot surrender the absentee ballot, that voter may be issued a provisional ballot.
- b. Voted Ballot Sealed: If a voter returns a voted absentee ballot, verify that the ballot is sealed and that the signature of the voter is on the identification envelope.
- c. The poll worker, once verifying the voter on the polling roster, is precluded from notating the date and

time the voter has voted on a device.

d. After the voter's name is checked off the roster, they will be given a Voter Access Card. A voter access card is created using either a AccuVote-TSX, Voter Card encoder, or VCProgrammer. A voter will be provided instructions on using the AccuVote-TSX.

e. The voter inserts the voter access card into the AccuVote TSX, and the system reads the voter access card for the appropriate ballot display

f. The voter inserts the Voter Access Card into the AccuVote TSX, and the system reads the card for the appropriate ballot display.

g. The voter selects the ballot choices and reviews those choices on the AccuVote-TSX summary screen.

h. The AVPM audit paper trail will generate a paper summary of their ballot selection to verify against the on-screen summary of the ballot. The voter has the ability to accept or reject the on screen summary.

i. Upon casting the vote, the AVPM paper audit trail results are stored on both the removable media and the flash memory. The AVPM audit trail is automatically taken up into the security canister. After touching the "Cast Ballot" button, the public counter and protective counter is incremented. Redundancy provides a check and balance where the numerical count of both files must match.

j. The electronic results are stored electronically in a random order.

k. After recording the ballot, the voter access card is disabled.

l. Whenever the system is in use, the audit log is activated.

m. Upon completion of all audit checks, the next voter is allowed to proceed with making selections and casting his/her ballot.

AccuVote-TSX Privacy

Arrange the AccuVote-TSX units, wherever and whenever possible to provide voters with a private voting environment.

In jurisdictions where the main voting method is paper and the AccuVote-TSX is used only for ADA accessibility, the poll workers may allow non-ADA voters to vote on the AccuVote-TSX to provide additional votes and paper audit trails to the AVPM and to guarantee anonymity for the voters.

Voters who leave the booth without printing their ballot or casting their ballot ("Fleeing Voter") will have their voter access card ejected and their vote not counted. There is a 30 second time out message that will appear on the screen after a period of 2 minutes of inactivity. The screen will count down from 30 seconds, and will allow the voter to resume voting by pressing the "resume" button, or the countdown will continue to 0, at which time the voter access card is ejected and the ballot is cancelled.

If the voter allows the AccuVote-TSX to time out, a new voter access card will need to be coded.

For the AccuVote-OS

a. The poll worker, once verifying the voter on the polling roster, is precluded from notating the date and time the voter has voted on a device.

b. Instruct each voter in the proper method of voting by filling in the oval, casting write-in votes and using the secrecy sleeve. Each voter shall be given further instruction and practice time with a demonstration ballot, if necessary.

- c. Write-in space is provided on the ballot. The voter must both write the name of the candidate and fill in the voting position oval for the vote to be counted by the AccuVote-OS.
- d. Instructions in inserting voted ballots into the AccuVote-OS shall be given after the voter has completed voting, if necessary.
- e. Check periodically to make sure the AccuVote-OS is working properly.

Left Side Auxiliary Bin of the AccuVote-OS

The Left Side Auxiliary Bin of the ballot box may be used as a storage area, if none has been provided, for the temporary storage throughout Election Day for these ballots:

- Delivered, voted Absentee Ballots;
- Surrendered Absentee Ballots, unless directed otherwise by the Election Official;
- Voted Provisional Ballots;
- Voted Ballots that will not be accepted by the reader;
- Ballots voted during emergency periods.

During the time when the polling place is open, the results tape shall not be removed, nor shall any portion of the results tape be torn off.

If for any reason the AccuVote-OS becomes inoperative, voting will continue. From the time the device becomes inoperative, until is the AccuVote-OS is made operable or replaced, voted ballots shall be placed in the Left Side Auxiliary Bin. If, and when the AccuVote-OS is restored to operation, a precinct officer, if approved by the election official or authorized designee, witnessed by a second precinct officer shall enter ballots, which have been stored temporarily in the Left Side Auxiliary Bin, into the AccuVote-OS. This process shall neither hinder nor delay voting, and shall be performed during inactive voting periods, or after the last voter has voted and before the “Ender Card” is processed. During this process, if a damaged ballot is encountered, it shall be placed in an envelope or container appropriately labeled. Such ballots shall be held by the Election Official for inclusion in the Final Official Canvass.

5.5 Special Needs Voters

For AccuVote-TSX Precincts – Voter Assistance

The AccuVote-TSX VIBS is designed for use by voters with a wide variety of disabilities. When a blind voter is using the AccuVote-TSX, the poll worker or blind voter’s assistant shall place the VIBS cover on the AVPM printer housing. The VIBS cover and the blank AccuVote-TSX screen will provide the blind voter privacy when using the AccuVote-TSX in VIBS mode. The Voter may be assisted with inserting the Voter Access card if necessary as well.

The poll worker can also assist in adjusting the angle for the AccuVote-TSX for the voter prior to the voting process. Additionally, the voter has the option of selecting a high contrast screen, or the large font screen to enhance the text. Voters should be given a large magnifier, if needed, to magnify and see the contents of the AVPM window.

For a blind voter, the VIBS kit can be used to provide audio functionality. The audio is played for them to make their selections. With the option to have the screen completely blank to ensure their privacy even with an assistant standing near by, blind voters are able to listen to an audio ballot and make their selections with the keypad. The 5 key, with its raised dot, is used to select and de-select races and candidates when their names are read.

Voters with Limited Dexterity may use the tethered keypad on the AccuVote-TSX which can be placed in their lap for use without the need to raise their arms. The adjustable screen angle enables them to position themselves close to the touch screen. The voter could also utilize a mouth stick to touch the screen.

For AccuVote-OS Precincts – Voter Assistance

A precinct officer shall be available near the AccuVote-OS device for assisting voters. Secrecy sleeves should be utilized to protect the voter's privacy. This officer may be on the board of any precinct, if Multiple Precinct Processing is implemented. The same officer does not necessary need to perform these duties throughout the day. Those duties may be rotated between each precinct.

- a. Make sure the voter stub has been removed from the ballot and given to the voter. Assist the voter, if requested, in how to insert his/her ballot. An Assisted Voter affidavit does not need to be completed unless the assistance requires the viewing of the voting positions on the voter's ballot.
- b. Read and inform the voter of the text of messages displayed by the LCD, if any.
- c. Inform the voter of what corrective action, if any, may or must be taken, or inform the voter of what options, if any, may or must be chosen.
- d. When assisting the voter as described above, the precinct officer shall position him / herself, so that the voted portion of the ballot shall not be in that officer's view.

5.6 Provisional Voters

For the AccuVote-TSX

Paper provisional ballots may be issued at the polls according to the prescribed state laws. The AccuVote-TSX Ballot Station is capable of separating provisional ballots from non-provisional ballots. When a voter appears at the precinct and is identified as a provisional voter, the AccuVote-TSX ballot station software identifies the voter's ballot, so that it can be retrieved, should the voter be determined eligible or ineligible by the canvassing board. In order for that ballot to be retrievable, the provisional voter is processed and assigned a voter ID number. The voter's provisional ID number is stored in the voter access card by the poll worker along with the voter's precinct and ballot style information. The voter proceeds to the AccuVote-TSX Ballot Station, inserts the voter access card, votes and casts the ballot, and returns the voter access card for re-use by the polling place.

The provisional ballot is recorded but not added to the result totals. Should the provisional voter's ballot be determined to be eligible for counting by the Election Board during the post election canvass, it would be identified in the election system by the provisional voter's ID number, and retrieved and added to the election result totals. This process is accomplished in GEMS on the challenged ballot screen, where the provisional voter's ID number is located. The GEMS administrator has the option to "accept" or "reject" the provisional ballot.

When electronic provisional (challenge) voter ballots are used, they will be identical in form as official electronic ballots. In lieu of electronic provisional ballots, paper provisional ballots may also be allowed. Provisional voter ballots are to be used at all elections by voters who claim to be registered but whose right to vote cannot be immediately established. If a voter's eligibility to vote cannot be established, the election official uses the Voter Card Encoder to designate the provisional (challenge) voter and load the applicable ballot, and the provisional voter's results will then be automatically isolated by the AccuVote-TSX system for resolution after the election. Procedures should be established to reconcile, count and / or reject the appropriate Provisional ballots cast electronically; these procedures should be in place for Paper Provisional ballots as well.

For the AccuVote-OS

Paper provisional ballots may be issued at the polls according to the prescribed state laws. The procedures for issuing a paper provisional ballot are the same as an AccuVote-TSX precinct in that the provisional voter will be assigned a provisional ID number. The provisional ID number will be on the voter's provisional ballot envelope. The provisional ballot will be adjudicated during the post election canvass process by a jurisdiction's canvass board, or by authorized members of the jurisdiction's staff.

5.7 Closing the Polls and Vote Reporting

For the AccuVote-OS

Closing the polls shall be conducted as prescribed in Election Code Section 14401 et. seq.

The Following Procedure must be completed in Public View:

- 1 Promptly at 8 p.m. declare, "The polls are closed". Any voter in line at the time of closing must be allowed to vote. No voter who arrives after 8 p.m. may vote.
- 2 Precinct Voter Ballots: The AccuVote-OS will have a total number of ballots counted on the Results Tape. Keep the ballots with the write-in votes separate from other ballots.

3. Process Voted Ballots: All ballots cast at the polls and counted through the AccuVote-OS in the precinct are counted, except for the write-in votes. All of the cast ballots should be reviewed for valid write-ins. Upon inspection, if there are write-in vote(s), no further action is required. Place the ballot cards with write-in votes within a precinct in one stack.

Ending the Election

Following the close of the polls, the precinct board shall remove any and all voted ballots from the Left Side Auxiliary Bin that were not counted by the AccuVote-OS. The precinct board may attempt to feed these ballots into the AccuVote-OS for counting, or return those ballots to the central election office for processing. Those ballots that continue to be rejected by the AccuVote-OS should be placed inside the designated container as directed by the Election Official and sealed.

The precinct board shall unlock and remove the printer cover of the AccuVote-OS device, then obtain access to the front of the AccuVote-OS by unlocking the top front door of the ballot box. While holding the YES and NO button on the front of the AccuVote-OS at the same time, insert the Ender Card into the AccuVote-OS. This will initiate the FINAL Results Tape that will print automatically. If the tape does not print, call the Election Official immediately. The printed tape will include both the ZERO TOTALS TAPE and the FINAL RESULTS TAPE. The precinct board shall tear the tape from the AccuVote-OS and return it to the Election Official as specified.

The precinct official shall print two copies of the audit log and two copies of the election summary report from the AccuVote-OS and post one copy of each report at the polling place. The other copies shall be returned to the central elections office. The poll workers must sign the reports. The precinct board also records the ballots cast total on the Precinct Ballot Statement as directed by the Election Official.

After printing the final results tape, the precinct board returns the AccuVote-OS memory cards to the Election Central for direct upload to the GEMS Server. THE MEMORY CARD SHALL NOT BE REMOVED FROM THE ACCUVOTE-OS UNIT EXCEPT BY AN AUTHORIZED ELECTION OFFICIAL which may include poll workers, county officials and couriers. There shall be two people transporting the memory cards from the precincts to the accumulation center / election office at all times.

Examine the Ballot Bins: Any delivered voted absentee ballots shall be placed in the designated container provided for that purpose. Place any surrendered absentee ballots in the designated container provided for that purpose. Place any voted provisional ballots in the container provided for that purpose.

The Precinct Board will remove all of the voted ballots from the ballot box. The Precinct Board will place voted ballots into envelopes or containers and seal with the seal provided for that precinct. Also, the write-in ballots from the center compartment of the ballot box will be removed and place in an envelope or container as directed by the Election Official.

For the AccuVote-TSX

The Following Procedure must be completed in Public View:

Promptly at 8 p.m. declare, "The polls are closed". Any voter in line at the time of closing must be allowed to vote. No voter who arrives after 8 PM may vote.

Ending the Election

- On all AccuVote-TSX units, insert the Supervisor card.
- At the supervisor screen, enter the assigned Personal Identification Number to enter the supervisor screen, and then press the “OK” button.
- Press the End Election button.
- Open all AVPM units with the AVPM key and follow the county procedures for printing the report tapes. Poll workers are not allowed to break the security seal on the AVPM security canister and remove the tape housed within the AVPM security canister.
- At the report prompts, press the print buttons according to poll worker instructions. Print two copies of the audit log and two copies of the election summary report from the AccuVote-TSX and post one copy of each report at the polling place. The other copies shall be returned to the central elections office. The poll workers must sign the reports.
- At the prompt, use the key to open the side cover on all units (remove transport media if election is ending) and turn the AccuVote-TSX power off. Unplug the AccuVote-TSX and close the booth.
- If necessary, follow the county procedures for upload accumulation.
- Seal the PCMCIA card(s) in the designated envelope for transport. Count to make sure there is a PCMCIA card for each AccuVote-TSX Ballot Station. There shall be two people transporting the memory cards from the precincts to the accumulation center / election office at all times.
- Collect any absentee voter ballots or paper provisional voted ballots, if used.
- Complete all relevant paperwork as required by the jurisdiction and seal in appropriate containers for return to Election Central. Packaging for Return
- Package AVPM security canisters as directed by the Elections Official.
- Package AVPM printer housing and paper roll as directed by the Elections Official.
- Package or seal all other supplies, as directed by the Elections Official.
- Verify that the required materials have been placed into the appropriate container(s), listing the materials inserted in each container and indicating that the container(s) were appropriately sealed.
- Return all transport media, paper ballots and supplies as directed by the elections official.

Returning Voted Ballots and Materials

Return all ballots and supplies as prescribed by the Election Code and as directed by the Election Official. (EC §14430-1435; 15550-15551; 17301-17306 (2005))

5.8 Securing Audit Logs and Backup Records

Procedures should be in place to insure that all audit logs are retrieved and retained and back up copies of all records should be retained as part of the official election. This includes the printing of the audit logs for the AccuVote-OS and AccuVote-TSX following the election and posting those audit logs at the respective polling places. Audit logs from the AccuVote-OS and AccuVote-TSX units should be retained and may be printed at the elections office as part of the semi-official canvass. The audit logs from the GEMS server should be printed and retained as part of the official records for the time period required by law.

5.9 Troubleshooting and Problem Resolution

Troubleshooting the AVPM

If the AVPM does not work properly due to paper jam, or the paper record is unreadable during the course of a voter verifying the paper audit trail, the poll worker will determine whether the voter has completed casting the voter's ballot. If the ballot has been cast, the poll worker will close the AccuVote-TSX for voting, until the issue is resolved. If the voter has not completed voting, the poll worker will cancel that existing electronic ballot and create a new voter card for the voter, sending the voter to another AccuVote-TSX unit to complete voting.

The poll worker will contact the county elections office for assistance and report the problem.

A new security canister and paper roll may be loaded into an AVPM, if it is determined that the printer is functioning, but the paper was jammed or the printer cover was not firmly locked in place to allow the print to be visible on the paper. If it is necessary to replace the security canister with a new one, the canister in the AccuVote-TSX at the time of the jam will be placed in the poll worker's election return supply bag or designated container and stored by the precinct captain / inspector until the close of polls. The canister will be returned with the election AccuVote-TSX units and supplies to the central location. The poll worker will make effort to insure the privacy of the voter's ballot.

If the AccuVote-TSX is the sole unit in the precinct and the voter is an ADA voter, a paper ballot could also be issued for assisted voting, if requested by the voter, if the AccuVote-TSX is closed.

If the AVPM is running low on paper, and the message indicating the paper is low is displayed, the poll worker will not allow voters to vote on that AccuVote-TSX until the paper roll and security canister is changed. The poll worker must use a new security canister and paper roll, take the old security canister and place it in the designated election return bag.

If the paper low message appears and it does not appear that the paper is low, the poll worker should verify the message by the opening the AVPM and if the paper is fine they will need to insert the Supervisor card to resume voting.

If the voter access card is ejected and the message appears that it was inserted upside down or incorrectly – the voter should notify the poll worker – the poll worker will reinsert the card in the AccuVote-TSX to verify and issue the voter a new card if necessary.

If a paper jam or the paper low message appears, and it appears that the paper has been misfed by a poll worker, the poll worker will contact the elections office for assistance. If the jam occurs during voting, the poll worker may be instructed to cancel the ballot and provide the voter with a new voter card. If the AccuVote-TSX is the sole unit in the precinct and the voter is an ADA voter, a paper ballot will be issued for assisted voting.

At no time will the security canister be opened to resolve a paper jam. It may be necessary to use a new security canister to resolve the paper jam. The poll worker will install the new security canister, take the old security canister and place it in the designated election return bag. At no time should the poll worker break the security seal on the security canister or open the old security canister.

If a paper jam occurs during the printing of the zero report, the security canister may be opened to resolve the paper jam, and then a new security seal would be put in place with the security seal number recorded. The security canister may not be opened if there are official election paper ballot audit trails in the security canister.

For AccuVote-OS Precincts

Some possible problems and their resolution are included below:

- NO Ballots -Inspector lost ballots/Car Crash, etc: A poll worker will have reported this problem to the office or hotline troubleshooting desk. The precinct inspector will be informed regarding whether to pick up ballots and where or whether they are to be delivered to the polling place.
- Can't Locate Ballot Box: The hotline troubleshooting desk will encourage the precinct inspector to continue looking for the ballot box. If they can't find it, the hotline troubleshooting desk could look in the jurisdiction warehouse to see who delivered and where they put the ballot box. If there is still no ballot box, the hotline troubleshooting desk will dispatch a ballot box to the precinct. The poll worker will be instructed to have the voters deposit voted ballots in "temporary ballot box" using AccuVote-OS bag, designated container or a ballot transfer bag.
- Forgetting to Bring AccuVote-OS: Until the problem is resolved, have the voters will deposit ballots in the side auxiliary bin of the ballot box. If this scenario happens, open the Left Side Auxiliary door (emergency slot) on the side of the ballot box with the keys that you have in the troubleshooter AccuVote-OS bag. Voting can proceed, with voters depositing ballots in the side auxiliary bin, while the Inspector sends to obtain, or an AccuVote-OS arrives at the polling place.
- Lost AccuVote-OS / Automobile Accident, etc.: Until the problem is resolved, have the voters deposit the ballots in the left side auxiliary bin of the ballot box. Immediately call the hotline troubleshooting desk and let them know the polling place name needing the AccuVote-OS. Make arrangements to have AccuVote-OS with the memory card delivered in the most expedient manner (meet delivery person half way), or you may need to return to the Elections Office building to get an AccuVote-OS. When you get The AccuVote-OS at the precinct, it will already be in "election mode" and you will simply insert turn the AccuVote-OS on, following opening instructions. Explain to inspector that ballots in the side bin should be processed prior to running the ender card at the end of the day.
- Can't Close front door of Ballot Box: Occurs when the small arms in the top door are not lining up with holes on side of ballot box. Try having another poll worker help pull the AccuVote-OS back while trying to lock front door. If this doesn't work, they can operate AccuVote-OS with the front door down, until troubleshooter arrives.
- AccuVote-OS won't slide completely into ballot box: It is possible that the ballot box connector is not mating properly with the AccuVote-OS receptacle. This connection is used to run the ballot box diverter arm for sorting ballots. If the pins are bent on the ballot box, straighten them and try again. Sometimes the AccuVote-OS needs to be lifted very slightly while mating with the ballot box pins.
- Memory Card reads "OK to Format? " when AccuVote-OS is turned on: Until the problem is resolved, have the voters deposit ballots in the left side auxiliary bin of the ballot box. You can try pulling out the memory card and re-inserting it into the AccuVote-OS, and turn on AccuVote-OS again. Try this approach up to five (5) times. Sometimes the card is OK, but in traveling is loose and making bad

connection. IF CARD STILL DOES NOT WORK, call the hotline troubleshooting desk and let them know the polling place name and that they will need to burn a new memory card for the precinct. Make arrangements to have memory card delivered in most expedient manner (meet delivery person half way), or you may need to return to the Elections Office building to get a memory card. When you get the new memory card at precinct, it will already be in "election mode," and you will simply insert it into the AccuVote-OS at the polling location. When you turn on the AccuVote-OS, it will print the zero totals tape. Follow the remainder of opening instructions.

- Memory Card reads "Generating Report" but is not printing zero tape: Check to ensure the print ribbon is properly set in the AccuVote-OS. If this doesn't correct the problem, have voters deposit ballots in the left side auxiliary bin of the ballot box. Call the hotline troubleshooting desk and let them know the polling place name.
- No Opening / Closing Instructions: The hotline troubleshooting desk can try and walk the inspector through the opening procedures over the phone or have the voters deposit ballots in the left side auxiliary bin until the troubleshooter arrives. When troubleshooter is on-site, give the inspector spare instructions from the troubleshooter bag, and help them open the polling place.
- "No Keys" in AccuVote-OS bag: The hotline troubleshooting desk will ask the poll worker to re-check the AccuVote-OS bag, including all pockets in the AccuVote-OS bag. If there is still no key, the hotline troubleshooting desk should instruct the poll workers to use a ballot transfer bag or an AccuVote-OS bag as a temporary ballot box until the troubleshooter arrives. Have the voters continue voting, but deposit the ballots in a temporary bag or designated container.
- Key doesn't fit locks: The hotline troubleshooter desk can try and determine whether the inspector has two ballot box keys or two AccuVote-OS keys instead of one of each. If the inspectors have two (keys) that are the same, they can not open the polling place.
- If two ballot box keys: Have them open the Emergency / left side auxiliary bin and have the voters deposit the voted ballots here until the troubleshooter arrives. Until the problem is resolved, have voters deposit the ballots in the left side auxiliary bin of the ballot box. The troubleshooter will have to replace the keys when they arrive and then run the opening procedures per instructions. Instruct the inspector to run ballots from the emergency bin at end of day, prior to running the ender cards.
- Swapped black rubber key identifier: The hotline troubleshooting desk should also verify that perhaps the black key ring was placed on the wrong key, and they are simply trying the wrong key. If the inspector has one of each key type, it should work. If the inspector can't open poll, then the inspector will have to follow the "No keys" instructions above.
- If two AccuVote-OS keys: The inspector can't open polling place with ballot box. See "No Keys" above.
- 1st Ballot Won't go into AccuVote-OS: Verify that the ballot feed path is clear into the ballot box. The ballot slot may have the key positioned, so the lock arm won't allow the ballots to pass into ballot box. If so, insert the key into lock at ballot feed path and reposition lock arm.
- Printer jam: The troubleshooter should explain to the inspector to answer NO to need another copy during the opening instructions, and proceed with voting in a normal fashion. Replace and lock the AccuVote-OS printer cover until the troubleshooter arrives. The troubleshooter will reload the paper and ready it for the closing of the polls. The Audit trail on the memory card will show that the zero totals were run and the time they were run, so all voting will be accomplished normally without further problems.
- "Power Failure" flashing: The AccuVote-OS is not getting power and is running off the battery. It will operate approximately 2.0 hours without power. The hotline troubleshooting desk will first check the following:
 - Determine whether the AccuVote-OS is plugged into a wall outlet;
 - Determine if it is plugged into wall outlet that doesn't work (plug lamp or something into it to test outlet or just move it to another outlet;

- Determine whether the power strip switch is turned to off setting;
- Open the top door on ballot box, and gently slide the AccuVote-OS out far enough to see if power cord is still plugged into AccuVote-OS. If not, push it in firmly and relock front door of ballot box, and continue voting;
- If the AccuVote-OS is still not working, dispatch a troubleshooter. The troubleshooter will figure out the location of the hot outlet, check all connections, or may need to replace the power cord. The troubleshooters will be given a spare power cord with the AccuVote-OS.
- **"LOW Battery" Message:** This message displays that the battery needs charging. Perhaps the on/off switch was turned on somehow during transporting the AccuVote-OS. The hotline troubleshooting desk can tell the poll worker that the battery should charge up in a few minutes, assuming that there is power getting to the AccuVote-OS. Verify all connections are good. Tell the poll worker to open the emergency / left side auxiliary bin and deposit the voted ballots in the bin for approximately 10 minutes. Recheck the message display on the LCD. The message should be gone at this point and normal ballot processing can resume. Remind the poll workers to run the ballots in side bin prior to running the ender card. Tell the poll worker to call back if problem continues. If the problem continues, contact the hotline troubleshooting desk.
- **Ballot Jams:** The hotline troubleshooting desk will instruct the inspector to have the voters deposit the ballots in the left side auxiliary bin of the ballot box until the problem is resolved. The hotline troubleshooting desk will try and determine if problem is a "returned ballot" or a "counted ballot" (see error message section below).
- **"Returned Ballot Jammed in Reader":** If a ballot has jammed while it was trying to return it to the voter, the inspector should gently pull the ballot out of the AccuVote-OS (if they can access it from the front), or lower the front door of the ballot box, gently pull the AccuVote-OS out enough to see the jammed ballot from the rear of the AccuVote-OS, gently pull the ballot out, and relock the AccuVote-OS into ballot box. Resubmit the ballot.
- **"Counted Ballot Jammed in Reader":** If the ballot has jammed while it was trying to drop into the ballot box, the inspector should gently pull the ballot out of the AccuVote-OS (if they can access it from the front), or lower the front door of the ballot box, gently pull the AccuVote-OS out enough to see the jammed ballot from the rear of the AccuVote-OS, and gently pull the ballot out. The ballot should be manually inserted into the ballot box through the normal ballot slot path. Once completed, relock the AccuVote-OS into the ballot box. Unlock the bottom front lock on the ballot box and lift the ballot box lid. Look inside the ballot box (with any witnesses watching) and see if the ballots are caught on the diverter arm, or stack so that ballots can not fall into ballot box correctly. Fix any stuck or piled ballots.
- **If jams are happening often:** The ballot box may have ballots piling up in the ballot path, preventing them from dropping in the ballot box bin. If this scenario happens, the troubleshooter, will unlock the bottom front lock on the ballot box, lift the lid, and determine how best to fix ballots that get caught in diverter arm or stuck.
- **NO Ender Card:** The ender cards have been placed in the AccuVote-OS bag in a pouch on the bottom half of the bag. This pouch is under the AccuVote-OS when they open up the bag. Poll workers may not notice this pouch. If the poll worker does not have an ender card, contact a troubleshooter in the field, or dispatch a troubleshooter to the site. The troubleshooter(s) will have Ender Cards, and when he / she arrives, they can assist with the AccuVote-OS closing procedures.
- If it is late to obtain an ender card, instruct the poll worker to take the AccuVote-OS to the designated regional site drop off and explain to the regional personnel that they were unable to complete the closing procedures with the AccuVote-OS. The regional personnel can run an Ender Card and transmit results from the regional site.

Absentee/Mail Ballot Procedures (central tabulation)

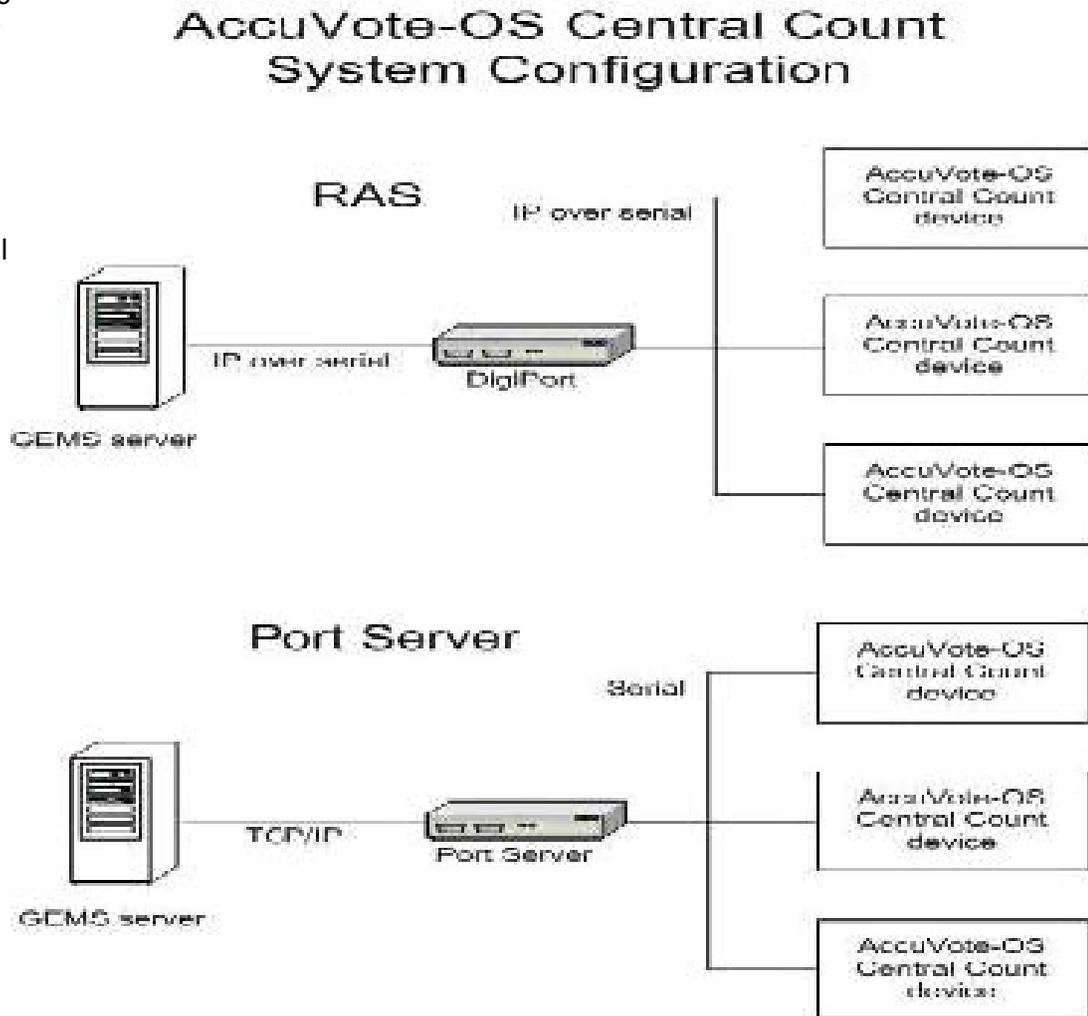
The AccuVote-OS Central Count is a batch ballot processing solution employing the AccuVote-OS ballot counting device configured with Central Count firmware, linked over a closed loop, local area network connection to the GEMS election management server.

The AccuVote-OS Central Count is useful for processing large volumes of mail ballots, such as absentee ballots. The AccuVote-OS Central Count mode allows any ballot type to be fed into the AccuVote-OS without any presorting of ballots. All that is required is that the vote center in which ballots are counted is logically associated with all election precincts to the vote center in the GEMS software.

The AccuVote-OS Central Count may be configured with multiple AccuVote-OS Central Count units linked to the GEMS server in either the local area network configuration or using Windows Remote Access Server (RAS). The AccuVote-OS Central Count may be scaled to accommodate the number of units, decks, and deck sizes required, while Ethernet-based local area network transmission between AccuVote-OS Central Count units and the GEMS server assures instantaneous results posting.

The picture below illustrates a sample Central Count setup:

GEMS is used to drive AccuVote-OS Central Count from the Central Count Server console, which provides an automatic and current live ballot count as ballot processing is in progress. All



Central Count administrative reporting functionality is offered in real time by GEMS, including deck counts by report precinct, by deck, and by posting time.

The AccuVote-OS Central Count employs all ballot validation logic of the AccuVote-OS, including the validation of control marks, such as the card ID, Diagnostic, and timing marks, card ID/precinct association, precinct/vote center association, white levels, and ballot stock weight. Ballots may be fed into the AccuVote-OS in any one of four orientations – face up, face down, head first, and foot first. Only valid AccuVote-OS ballots will be accepted by the AccuVote-OS, as generated by GEMS, and printed in conformance with Premier's *Ballot Specifications Guide*. Ballots processed in the AccuVote-OS Central Count may equally be processed in AccuVote-OS Central Count, AccuVote-OS Precinct Count.

Every valid ballot type may be tested on the AccuVote-OS Central Count unit using Unvoted, Fully Voted, and Count Tests. No test counts are introduced as a result of the Unvoted and Fully Voted Ballot Tests, and any counts resulting from processing test ballots may be easily reset in the GEMS database prior to Election Day. Please refer to AccuVote-OS Central Count Users Guide for more detail on these tests.

In addition to these ballot tests available in Central Count mode, the AccuVote-OS Central Count firmware also supports the setup and diagnostics modes. The setup mode is used to configure the AccuVote-OS Central Count device for central counting, while Diagnostics Mode is used to perform diagnostics tests on the AccuVote-OS device, including verifying its ability to log on to the network, display information on the LCD, test system memory, the AccuVote-OS printer, the main serial port, the auxiliary serial port, and the card reader. Setup and diagnostic modes are detailed in the AccuVote-OS Central Count Users Guide.

6.1 System Startup and Pre-Tabulation Report Procedures

The detailed start up, running and tabulation procedures may be found in the Central Count Users Guide.

6.2 Tabulation Procedures

Central Count is driven from the GEMS Central Count Server console. This console is divided into three tabs: Machines, Decks and Log.

The Machines tab displays all machines that are currently actively counting ballots in Central Count mode, and includes the deck number, the Central Count AccuVote-OS IP number, the machine status, and the current ballot count in the deck. Only machines are displayed that are actively counting ballots.

The Decks tab displays the numbers of all ballot decks that have been counted, the completion time, and the total deck count.

The Log records all batch start and end transactions, as well as any batch processing error conditions that have arisen. Those log reports can be printed from GEMS.

Disabling the Central Count Server console does not clear any of the decks counted and recorded under the Decks tab. Centrally counted ballot decks may be deleted either by selecting the decks under the Decks tab, and clicking on the Delete button, or by resetting election results. Once the Central Count Server console has been readied, the Start button is disabled, and the Stop button is enabled.

Note that the Central Count Server console is modeless, that is, it may be accessed at the same time as the GEMS main window. The election status cannot be changed as long as the console is active. As ballots are being centrally counted, monitor AccuVote-OS Central Count units to verify that equipment idle time is minimized. Review the Log occasionally, ensuring that any error messages that may arise have been properly accounted for.

A jurisdiction shall upload data into the GEMS server from only one memory card at a time. Below are examples of alternative procedures that a jurisdiction may implement to ensure that only one memory card is uploaded at a time when more than one device is being used to upload memory cards:

- a One jurisdiction employee is assigned to physically initiate the upload of every memory card throughout the process, moving from one upload device to another. This employee shall not initiate the upload of more than one memory card at a time.
- b One jurisdiction employee serves as director of all operators of devices used to upload memory cards. The director authorizes one operator at a time to upload a memory card and waits for the operator to confirm completion of the operation before authorizing another operator to upload a memory card. No operator may upload a memory card before receiving authorization from the director.
- c After the first memory card is uploaded, each memory card upload device operator uploads a memory card only after the operator to his or her right signals completion of the operator's memory card upload. This process continues until the last operator signals completion of his or her memory card upload, at which time the first operator begins a new cycle of memory card uploads.

Any decks that have been counted in previous central count sessions are listed under the Decks tab only once central count has been activated for the vote center under the Machines tab.

Careful reconciliation logs should be maintained daily to account for all ballots processed.

6.3 Post Tabulation Report and Shutdown Procedures

The central count reconciliation should occur immediately after shutdown to assure the jurisdiction that the correct number of ballots has been tabulated.

The central count reports from GEMS in the Administrative reports screen should be used to reconcile deck numbers with actual ballots processed and any discrepancies investigated.

These include:

- Central Count Status Report by Deck
- Central Count Status Report by Time
- Central Count Status Report by Race
- Central Count Status Report by Report Precinct

7. Semi-Official Canvass Tabulation and Reporting

7.1 System Start-Up and Pre-Tabulation Reports

The Election Official responsible for the conduct of an election shall assign staff or appoint canvass boards to carry out the following semi-final official canvass functions:

- a. Absentee Voter and Provisional Voter Ballot Processing
- b. Seal and Container Inspection
- c. Ballot Processing
- d. Ballot Duplication
- e. Memory Card Control and Processing
- f. Elections Observer Panel
- g. Other boards deemed necessary by the responsible election official. Individuals appointed may perform more than one function, or serve on more than one board
- h. Print the following reports from GEMS prior to shutting down and backing up for the evening:
 - Election Summary Report
 - AccuVote-TSX status report
 - AccuVote-OS status report
 - Cards Cast report
 - AccuVote-TSX write-in reports
- i. After printing the reports listed above and prior to submitting your final results to the Secretary of State on election night, each jurisdiction must verify for each precinct tabulated that a precinct total is listed on the Cards Cast report.

A jurisdiction shall upload data into the GEMS server from only one memory card at a time. Below are examples of alternative procedures that a jurisdiction may implement to ensure that only one memory card is uploaded at a time when more than one device is being used to upload memory cards:

- a ○ One jurisdiction employee is assigned to physically initiate the upload of every memory card throughout the process, moving from one upload device to another. This employee shall not initiate the upload of more than one memory card at a time.
- b ○ One jurisdiction employee serves as director of all operators of devices used to upload memory cards. The director authorizes one operator at a time to upload a memory card and waits for the operator to confirm completion of the operation before authorizing another operator to upload a memory card. No operator may upload a memory card before receiving authorization from the director.
- c ○ After the first memory card is uploaded, each memory card upload device operator uploads a memory card only after the operator to his or her right signals completion of the operator's memory card upload. This process continues until the last operator signals completion of his or her memory card upload, at which time the first operator begins a new cycle of memory card uploads.

All applicable reports should be assembled and be available. The procedures should be in place to reconcile precinct returns, absentee returns, and provisional ballots. Provisional ballots and any absentees from the polls may be prepared for resolution and presentation to the Canvass Board.

The Election Official shall establish procedures to account for all voted ballots, results tapes, security canisters, memory cards during the semi-final official canvass.

The Write-in ballots should be validated to those valid write-in candidates.

Absentee Voter and Provisional Voter Ballot Processing:

Absent voter ballots and provisional voter ballots, returned on Election Day, are sealed in designated containers by precinct boards for return to the designated counting location. These designated containers shall be stored in a secured location until such time as they are removed from the precinct supply kits. The condition of these seals shall be inspected and any defects noted and reported as required by the elections official.

Ballot Duplication

Correcting or duplicating defective ballots shall be done in a clear, unambiguous, and auditable manner such that the voter's mark and intent is preserved and the Election Official's action adheres to the voter's intent. For defective absentee or mail ballots and / or ballots where the voter intent is clear, but the AccuVote-OS cannot read the ballot, the ballot shall be processed according to the following procedures (defective ballots may be duplicated before processing or after rejection by the AccuVote-OS units, or both).

- 1 When an absentee or mail ballot voter takes corrective action on their ballot and voter intent is clear, the Election Official may use a Post-it Correction & Cover-up tape in lieu of duplicating a complete ballot to cover extraneous marks made by the voter or to allow the Election Official to enhance a mark made by the voter. The Election Official may make a designated unique mark on the tape so long as the tape could be removed and the original mark made by the voter is preserved. The Election Official shall initial next to this correction in an area in which it will not be interpreted as a vote.
- 2 When an absentee or mail ballot is insufficiently marked and the voter's intent is clear, e.g., ballot ovals filled in with red ink, light pencil or other light marks, then the ballots are to be duplicated or corrected following either or both of these procedures:
 - a) The Election Official may use a Post-it Correction & Cover-up tape lieu of duplicating a complete ballot to cover marks made by the voter or to allow the Election Official to enhance a mark made by the voter. The Election Official may make a designated unique mark on the tape so long as the tape could be removed and the original mark made by the voter is preserved. This unique mark or enhancement shall take the form of a slash mark on the tape covering the original oval the voter has indicated. The Election Official may make the mark so that it is sufficiently different in color and style and cannot be mistaken as the voter's original mark. The Election Official shall stamp or initial to this mark in an area on the ballot where the mark was enhanced by the elections official or authorized designee in which it shall not be interpreted as a vote.
 - b) The Election Official may use a colored translucent marker (such as a highlighter) that will not obscure, obliterate, or otherwise destroy the voter's original mark but will create a mark that is readable by the AccuVote-OS. The Election Official shall initial next to this mark in an area in which it shall not be interpreted as a vote.
 - c) When an absentee or mail ballot timing marks are defective, corrective active may be taken by duplicating the ballot and processing the ballot; or (2) repairing the timing mark.

Duplicating Defective Ballots.

Deliver defective voted ballots to the appropriate location for processing. All ballots prepared as duplicates of defective voted ballots shall be of a distinctive color, or be identifiable by other distinguishing means, clearly labeled "duplicate," and shall be given a serial number which shall also be recorded on the damaged ballot.

In creating the duplicate ballot, one board member shall duplicate voting positions marked on the original/damaged ballot, and shall enter a facsimile of the write-in vote(s), if any. Efforts need not, and should not, be made to match the handwriting characteristics of the voter when entering these write-in facsimiles. Particular attention must be paid to completing or not completing the ovals opposite the write-in spaces as the voter has done, or failed to do. Another member shall verify that the voting position marks and write-in entries (including oval completions or lack thereof) on the duplicate ballot match those in the damaged ballot.

Duplicates shall be placed with voted ballots of the appropriate precinct for further processing, tallying, and storage. The original ballot, which has been duplicated, shall be distinctively voided, placed in clearly identified containers for duplicated ballots, and segregated in a secure location so they cannot be counted inadvertently.

7.2 Processing Vote Reports

7.2.1 Central tabulation

All central count reconciliation logs and central count logs used for an election should be assembled and compared for accuracy. Errors and deficiencies should be investigated and resolved.

The central office will upload the memory cards from both the AccuVote-OS and AccuVote-TSX units. The elections official will report election results as specified by the local jurisdiction's reporting requirements and the Secretary of State's reporting requirements. See the *GEMS User Guide* for more information on uploading and reporting election results from GEMS.

8. Official Canvass and Post-Election Procedures

In order to assure the privacy of the voters, the County should establish procedures that assure the separation of duties between those who canvass the returns and those who work the polls.

The Official Canvass consists of a post-election audit of the voting 'precincts' returns and the absent voter ballot returns. The canvass is designed to:

- Validate the outcome of the election by verifying that there were not more ballots cast than the sum of the numbers of voters who signed the precinct Roster / Index, and who applied for and were issued absent voter ballots;
- Account for all official ballots produced for the election; to ensure that all required certificates and oaths were properly executed by the precinct board;
- Verify the accuracy of the computer count by manually recounting the voted ballots from at least one percent of the voting precincts and comparing the manually-tallied results to the computer-generated results;
- Process any provisional ballots;
- Process any valid write-in votes;
- Resolve any ballot exceptions;
- Certify the Election results.

8.1 Election Observer Panel

All procedures prescribed in this manual shall be carried out in full view of the public insofar as feasible. In addition, the responsible elections official shall devise a plan, subject to the approval of the Voting Systems Panel, whereby all critical procedures of the vote tallying process described in this Manual are open to observation by an Election Observer Panel. Representatives of the qualified political parties and representatives of the news media shall be among those invited to serve on this Panel and shall be given the opportunity to observe that the correct procedures have been followed in the receiving, processing, and tallying of all the voted ballots. The Election Official shall appoint an Election Observer Panel; failure of any or all invited parties to participate on the Panel shall not stop procedures from continuing as otherwise required by law.

8.2 Canvassing Precinct Returns

The processing of precinct ballots returned from the precinct during the canvass shall not be done by poll workers but by those appointed by the County Elections Official.

The recommended procedures for processing precinct ballots returned from the precinct during the canvass are as follows. This includes the return of precinct provisional ballots from the precincts.

- Verify eligibility of persons who cast ballots provisionally according to the Guidelines for Processing Provisional / "Fail-Safe" Ballots in an Election, as provided by the Secretary of State;
- Open envelopes of eligible voters and remove ballots;
- Examine ballots for write-in votes, noting cause for rejection and damage;
- Identify original or duplicate provisional ballots by precinct and deliver to the designated official for updating computer tallies;
- Write the reason for rejection on envelopes of ineligible voters. Place unopened envelopes with election materials to be retained for the period prescribed by law;
- Examine the Ballot Statement prepared by each precinct board;
- Compare the number of official ballots reported "received" by each precinct to the number issued by the elections official. Resolve or explain any discrepancy;
- Verify that the number of ballots voted (including those voted provisionally), plus spoiled and

unused ballot cards, equals the number received by the precinct. Resolve or explain any discrepancy.

Reconcile tallies

- Compare the number of signatures in the Roster-Index to the number of precinct voter ballots reported on the Ballot Statement. Resolve or explain any difference between the two;
- Compare the number of ballots voted by provisional and precinct voters to the Summary reports and/or results tapes. Resolve or explain any discrepancy;
- Locate any ballots not counted on election night because of damage, invalid identification marks, improper orientation, or any other reason;
- Search election supplies and equipment, including unused and spoiled ballots, write-in envelopes, ballot containers, etc., for ballots not accounted for.

8.3 Canvassing Absentee Returns

The elections official is accountable for absentee ballots to the same extent, as nearly as practicable, as for precinct ballots. The duties include:

- Prepare a Ballot Statement for each ballot type or special absent voter “precinct” showing the number of ballots produced (received), any defective ballots received from the vendor, spoiled or damaged ballots, the number of returned ballots that were challenged, and the number to be counted;
- Reconcile the statement to demonstrate that the total of unused, defective, spoiled, issued, and replaced ballots equals the number received. Resolve or explain any discrepancy;
- Updating absentee ballots returned on Election Day; and compare the computer count to the number of ballots to be counted, as shown on the Ballot Statement. Resolve or explain any discrepancy

8.4 Canvassing Provisional Ballots

The processing of absentee and precinct provisional ballots returned from the precinct during the canvass shall not be done by poll workers but by those appointed by the County Elections Official. The recommended procedures are as follows:

- Verify eligibility of persons who cast ballots provisionally according to the Guidelines for Processing Provisional/"Fail-Safe" Ballots in an Election, as provided by the Secretary of State;
- All AccuVote-TSX provisional ballots that require further investigation should be printed from GEMS and attached to the appropriate envelope to be processed according to established State Law and County procedure. All valid AccuVote-TSX provisional ballots shall be accepted in GEMS and the tallies updated;
- For AccuVote-OS provisional ballots, open envelopes of eligible voters and remove ballots;
- Verify eligibility of persons who cast ballots provisionally according to the Guidelines for Processing Provisional / "Fail-Safe" Ballots in an Election, as provided by the Secretary of State;
- Open envelopes of eligible voters and remove ballots;
- Examine ballots for write-in votes, noting cause for rejection and damage;
- Identify original or duplicate provisional ballots by precinct and deliver to the designated official for updating computer tallies whether those are paper provisionals;
- Write the reason for rejection on envelopes of ineligible voters. Place unopened envelopes with election materials to be retained for the period prescribed by law.

8.5 Canvassing Write-In Votes

All ballots containing write-in votes must be examined by the Write-In Processing Board or a board established by the county elections official and / or designee. The recommended procedures are as follows:

AVOS Manual Recount Procedures

The recommended procedures for the AVOS manual recount procedures for write-in votes are to examine the voting positions on the ballot for the office where the write-in vote occurs. The AccuVote-OS tabulator will have scanned each ballot and determined the oval markings for that ballot. If the write-in vote created an overvote condition, the ballot would have returned to the voter/operator for action. If the voter has marked the name on the regular ballot and written in the name on the ballot on the write-in line, the election official shall ensure that the vote is tabulated one time only. If the name is written in only and is not marked on the candidate list, the election official may determine the voter's intent to select the candidate.

- a. To be considered as a write-in vote, the oval next to the write-in space must be marked and /or filled-in (EC 15342).
- b. If the name written in is not on the Certified List of Write-in Candidates, the write-in vote shall not be counted.
- c. If the write-in vote is for a qualified candidate in the precinct and does not constitute an overvote, the write-in vote is manually tallied.

AccuVote-TSX Manual Recount Procedures

GEMS will indicate the number of votes cast for each write-in position for each contest. GEMS has the AccuVote-TSX write-in reports that will also contain the actual write-in candidate's name cast by the voter as recorded on the AccuVote-TSX units. Immediately after results are uploaded for AccuVote-TSX units, the GEMS database shall be backed up with the established naming convention. This will also be done prior to closing down the server at the end of the evening.

Prior to any reconciliation of qualified write-ins, the jurisdiction may (1) print the AccuVote-TSX ballot images from GEMS; (2) print the applicable write-in summary reports; or (3) tally the write-in totals from the AVPM.

The local officials will tally and record the write-in votes cast for write-in candidates from this report. In tallying the write-in votes in a contest designated as a "Vote for Two" or more, the election official may encounter a name written in that is the name of a ballot qualified candidate. In this instance, the election official shall check the ballot image report to determine whether the ballot qualified name written in is also marked on the list of candidates.

8.6 1% Manual Tally

For the purpose of validating the accuracy of the computer count, a public manual tally of 1% as required by the California Election Code of the ballots cast should be conducted as to all candidates and ballot measures voted on in each of the precincts.

For the manual tally, the AVPM paper audit trail and ballots shall be tabulated by hand using county established procedures.

The recommended procedures for counting on the AVPM are as follows:

- Print out the applicable precinct summary report in GEMS
- Print out the ballot images from the vote center that were uploaded and compare the actual AVPM record to the ballot images from GEMS to further validate the results, Or, manually tally the results from the AVPM and compare the tally to the precinct reports from GEMS. If the AVPM summary and the GEMS Summary are different, it must be determined if a manual counting mistake has occurred. If an error has occurred, the error must be reconciled.
- The County should take measures to assure an accurate manual count is conducted of the AVPM summary reports and no person who worked at that polling location should be allowed to conduct this count.

8.7 Handling Ballot Exceptions

The precinct and/or absentee ballots may contain writing or marks that could identify the voter. These ballots must be examined by the Elections Official. If the marks WOULD IDENTIFY the voter, the ballot should be rejected and placed it in the designated container.

Names, addresses, and initials are considered identifying marks. If the marks WOULD NOT IDENTIFY the voter, process the ballot along with all other valid ballots. The following specific standards shall be used in determining if one or more marks on an AccuVote-OS ballot are to be included in the count.

Marked Voting Position Oval

A vote shall be considered valid and included in the count when the marked voting position oval is completely filled in. Other Marked Ballots A vote shall be considered valid and included in the count when the voter has marked the ballot in a clear and understandable manner such that a pattern or patterns are discernable.

8.8 Post Election Logic and Accuracy Testing

A Post-Election Logic and Accuracy Test similar to the Pre-Election Logic and Accuracy Test may be performed following the election at the County's discretion.

Post-Election Logic and Accuracy Testing is addressed in the GEMS Election Administrator's Guide.

8.9 Final Reporting of Official Canvass

The official canvass consists of a post-election audit of the polling place returns and the absent voters returns and serves to;

- Validate the outcome of the election by verifying that there were not more ballots cast than the sum of the numbers of voters who signed the precinct Roster/Index and who applied for and were issued absent voter ballots;
- Ensure that all required certificates and oaths were properly executed by the precinct board;
- Prepare the Statement of Votes Cast Report (SOVC)
- Verify the accuracy of the computer count by manually recounting the voter ballots from the authorized recount requirements that include comparing the manually-tallied results to the computer-generated results and the paper audit trails.

The final results shall be verified and delivered to the Secretary of State in the manner prescribed by law.

8.10 Backup and Retention of Election Material

Upon the certification of the election results, Elections Code sections 17300 through 17506 apply to the handling, security and disposition of unused ballot cards and other elections materials. The retention period for ballots and related election materials is six months for all elections if no federal elections are involved. The federal election retention period is twenty-two months. The retention periods may be extended in the event of a court challenge. All ballot tabulation operations including mandated pre-and post-election testing, must be documented in sequential order. An automated and/or manual record or log must be maintained to record the time and date of "system events" related to ballot counting. All associated election materials must be retained for the period prescribed by law. Copies of the election database should be date and time stamped and preserved as well. They may be in the form of cd or other media.

System events in the ballot tabulation process include:

- Initiation of the ballot count program
- Clearing totals
- Running logic and accuracy tests
- Hardware Failures
- Repairing hardware (including running accuracy tests after repairs are completed)
- System crashes and restarts
- Communications between multiple systems
- Lost communication to remote sites
- Time communication is restarted

The GEMS Audit log shall be continued until final certification of results, shall be printed and retained for this same time period as ballots for that election, and shall be subject to the same physical security and integrity measures.

Specific audit trails may include:

- Exception Handling/Error Messages During Ballot Tabulation, such as;
- AC offline
- System status messages, such as:
- Polling Place Open and Close

See Section 10.6 for details regarding audit log management.

9. Recount Procedures

A request for a recount and the conduct of the recount shall be made in accordance with Elections Code section 15600 with the following:

Public Observation

The recount shall be conducted publicly.

Appointment of Spokesperson

Upon request, the elections official shall determine the candidates and or campaigns or others that are parties of interest in the recount, and each party of interest shall appoint a spokesperson who shall act as a contact person between the election official and the party of interest. The spokesperson shall be authorized by the party of interest to make final decisions on behalf of the candidate or campaign. The spokesperson shall have access to all parts of the recount area when accompanied by an Election Official. The spokesperson may appoint other persons to observe the recount process, the number and activities of such persons depending on procedures established by the Elections Official.

Order of Precincts

The person requesting the recount may specify the order of precincts to be counted, and may specify whether the recount begins with precinct ballots, absentee ballots, provisional ballots, or other types of ballots. In the absence of such a request, the elections official shall determine the order in which precincts are counted. Any change to the order must be requested in writing by the candidate or campaign, or the designated spokesperson.

Ballot Security

The elections official shall provide for the security of ballots during the recount process. The costs for any security measures in addition to those determined necessary by the elections official that are requested by the voter requesting the recount and that are approved by the elections official shall be added to the cost of the recount.

Cost of Recount, Daily Deposit

The voter filing the request seeking the recount shall, before the recount is commenced, deposit with the elections official a sum as required by the elections official to cover the cost of the first day of the recount. For subsequent days, no later than 3:00 pm the day before each day's recount, the requestor shall pay to the elections official a sum sufficient for the next day's recount, as determined by the Election Official. If the advance deposits are not paid, the Election Official will terminate the recount.

Examination of Ballots and Other Materials

Any research, review, or handling of relevant election material, as defined in Elections Code section 15630, shall be done at the discretion of the Election Official. Requests to research, review, or handle relevant materials must be in writing and must be received by the elections official before the recounting of ballots is complete. The requestor shall pay all additional costs to complete the research or review. One or more representatives of each party of interest, as determined by the elections official, may be present for any research or review of relevant materials conducted under this section.

Interference with the Recount Process

No person appointed as an observer may interfere with the recount process. All questions must be directed through the designated spokesperson directly to the elections official or his or her designee. No questions or remarks of any kind may be directed to any member of the recount board. No observer may touch or handle ballots.

Procedure to Challenge Ballots

Ballots may be challenged according to the provisions of Elections Code section 15631. The elections official shall, prior to the recount, establish a procedure for review and resolution of challenges. This procedure shall include, but is not limited to, notice to all interested parties of the rules, regulations, and procedures that will be used to resolve challenges.

10 Security

10.1 Physical Security of System and Components

Introduction

Physical security is paramount to running accurate and secure elections. As part of preparing for an election, each jurisdiction should review its physical security processes and procedures, and identify best practices for maintaining and improving those processes and procedures. This section defines some of the steps for each jurisdiction in establishing and maintaining procedures for physical security. The main goal for the elections official in maintaining these processes and procedures for physical security is ensuring the protection of the election tally process from intentional manipulation, fraudulent manipulation, fraudulent and intentional manipulation, malicious mischief, accidents, and errors. As part of ensuring physical security of the election system and components, each jurisdiction should:

- a. Procedures: System Changes — These procedures may also include a check list and sign-off requirement for the system (logic) proofing tasks.
- b. Procedures: Physical Protection — Establish procedures for the physical protection of facilities, and data and communications access controls as appropriate for the facility and equipment. The procedures shall also include provisions for locked facilities for computers as well as for voted and non-voted ballots and counted and uncounted ballots.
- c. Procedures: Technical Security – Establish procedures for the technical security of the system, including the establishment and maintenance of passwords, system and database backup, administrative privileges and access to those privileges, among others.
- d. Procedures: Internal Security — Establish procedures for internal security, i.e., the protection of ballot counting hardware, firmware, and software from fraudulent manipulation by persons within the elections office. These procedures should address:
 - 1 Restricted access to ballot counting hardware, firmware, and software;
 - 2 Develop processes for ensuring no malicious attack or tampering has occurred on the election equipment;
 - 3 Processes for a standalone election network protected from malicious attack or tampering;
 - 4 Individual passwords which must be complex and frequently changed;
 - 5 Physical protection of all non-voted precinct and absent voter ballots, as well as of all tallied and non-tallied ballots to chronicle their use and access before and after the election.
- e. Contingency Plan — Establish contingency plans for ballot counting, including either backup ballot counting facilities under the elections official's supervision, or a reciprocal agreement with a neighboring jurisdiction to count ballots in the event of hardware failure. This should include the development of a risk assessment plan to identify risks and disaster recovery plans in the event of a hardware failure. In addition to the ballot counting program sent to the Secretary of State, each elections official should store another copy of the ballot counting program in a secure-but-readily-accessible location.

A copy of each County elections official's security procedures should be on file in the office of the election official.

In addition to the above procedures, the jurisdiction should establish procedures to identify and certify individuals who may observe the ballot counting and tabulation process, pursuant to California election law. All unescorted persons present within the security area, including visitors, media representatives, and standby personnel, shall be clearly identified by a badge or other means and a log of their arrival and departure times. All unescorted personnel shall be subject to restrictions established by the responsible elections official to ensure the efficiency, transparency and integrity of the vote tallying process.

Election Security Plan

Each jurisdiction should develop an Election Security Plan that addresses the following areas of security. The areas of security include the ballot tabulation program, the precinct counting system, and other peripheral systems and components. The following areas are recommendations based on prior recommendations for improving security of the ballot tabulation system, and best practices for security of the ballot tabulation program.

Security of the Ballot Tabulation Program (GEMS server)

- 1 Election Officials shall maintain the GEMS Server is in a controlled, preferably locked area with access limited to authorized staff and personnel.
- 2 Access to the GEMS server shall be tightly controlled and all persons having access to the server at any time, shall be pre-approved by the county elections official and noted in a log that details the name, date and time of access to the room in which the GEMS is housed.
- 3 Election Officials shall verify that no Direct Access Oriented (DAO) capable program has been installed or resides on GEMS server. DAO programs include but are not limited to MS EXCEL, MS ACCESS, and other Visual Basic programs designed to work with Direct Access Objects.
- 4 The GEMS server shall be set to require user login. Administrative user logins should be limited to only those times user accounts need to be set or changed or software needs to be installed or updated. For routine use, a lesser user account should be used. An administrative user should also be issued an additional, separate user account for routine use if their duties require routine election use.
- 5 A minimum of two people in the county election office shall have administrative access to the server supporting GEMS (the ability to set or change passwords). Additional user accounts may be assigned at less than administrative access but all users shall have and use separate user account with unique usernames and passwords. The administrative users' passwords shall meet or exceed Microsoft Windows password guidelines for a strong password. Lesser user accounts should be at least as strong as the GEMS passwords. The second administrative user username / password should be stored in a sealed envelope placed in a safe as part of a disaster recovery plan but should not be used for routine use.
- 6 Network connections, including the GEMS network, should be local.
- 7 The GEMS server computer and communications systems shall be used for election purposes only.
- 8 Election staff shall not install third-party software on the GEMS server system that has not been previously approved for use by Premier.
- 9 Whenever software and / or files are received from any external entity, this material must be tested for unauthorized software on a standalone, non-production machine before it is used on the GEMS server system. If a virus, worm, or Trojan horse is present, the damage will be restricted to the involved machine.
- 10 Approved virus checking programs must be continuously enabled on computers supporting the GEMS server system. Premier recommends McAfee virus scan. The virus checking programs should be updated and a virus scan ran immediately prior to any election.
- 11 Externally supplied floppy disks, CDs or DVD's may not be used on any GEMS server unless these disks have first been checked for viruses and deemed to be free of such viruses.

12 If unofficial summary results from the GEMS server are to be distributed or published, the information should be exported from GEMS to a file on the server and then copied to electronic media (e.g., floppy disk, CD). That electronic media can be taken to a separate computer system that has external connections to the Internet for export.

13 Back-ups of GEMS databases should be performed using electronic media (e.g., CD). Users must ensure that the back-up is labeled with the time and date of the back-up and signed by the person who authorized and performed the back-up. Additionally, the GEMS election database should be backed up periodically.

14 No voting terminal or other component of the voting system will have wireless technology installed or have any ability to allow the transmission of vote results through wireless technology.

15 The boot option shall be set to hard drive only with the BIOS secured by a password. The password shall follow industry standards for a secure password.

Security of the Precinct Counting Systems

Security of AccuVote-TSX units

The following are areas for improving security of the AccuVote-TSX unit, and best practices for security of the AccuVote-TSX unit:

- 1 All AccuVote-TSX units shall be upgraded to use software that requires SSL/TLS standards and be documented.
- 2 New encryption keys using the Key Card Tool (KCT) shall be created and used for Administrative and Supervisor Smart Cards and AccuVote-TSX units for each election. These keys will be stored in a secure location with limited access by use of County election officials.
- 3 Security keys shall be verified and logged as they are changed.
- 4 No PIN shall use only the digits "0" and "1".
- 5 Each memory card shall have a permanent serial number assigned to it.
- 6 The county shall maintain a chain-of-custody log that accurately records the chain-of-custody of each memory card and AccuVote-TSX unit from the point of programming the memory card for use in the election through the time of completion of the official canvass.
- 7 The chain of custody log can be created for the county to record and track the serial number of each security seal placed on the AccuVote-TSX unit. The chain of-custody log would be used to verify the correct security seals are on the AccuVote-TSX, and have not been tampered. An example of a chain-of-custody log is below:

7. All AccuVote-TSX units shall be sealed across the halves of the unit with a serialized tamper-evident seal such that the unit cannot be open or disassembled without breaking the seal. A log shall be maintained of such seals assigned to each AccuVote-TSX unit. The integrity of that seal shall be verified after programming each AccuVote-TSX unit for an election, prior to opening the

TSX Chain of Custody Form								
District#: _____			Precinct#: _____		Precinct Name: _____			
County: _____				Election: _____				
OUT					IN			
TSX Serial Number	Privacy Panel Seal Number	Election Data Compartment (Upper) Seal Number	Election Data Transport Compartment (Lower) Seal Number	Transporter Initials (After Delivery)	Privacy Panel Seal Number	Election Data Compartment (Upper) Seal Number	Election Data Transport Compartment (Lower) Seal Number	Transporter Initials (After Return)
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
Designated Warehouse Personnel's Signature:					Designated Warehouse Personnel's Signature:			
Transporters' Name Printed:					Transporters' Name Printed:			
Date Picked Up:					Date Picked Up:			
Signature of Transporters:					Signature of Transporters:			

polls, immediately upon closing the polls, and upon return of the AccuVote-TSX unit to the jurisdiction's headquarters after the election. The authorized poll worker shall verify and validate the security seals have not been tampered prior to, and upon closing of the polls. The county may also choose to seal other areas of the AccuVote-TSX with tamper-evident seals for additional security. The chain-of-custody log shall be signed by the authorized poll worker.

8. If a violation of the tamper evident seal is discovered prior to the start of the election, the elections official or designated person will investigate and determine the appropriate course of action. If an elections official or designated person has determined a violation has occurred, the AccuVote-TSX unit shall be immediately taken out of service and the violation inspected by the chief election official or designated person and reported to the Secretary of State. If a violation of the tamper evident seal is discovered after the start of the election, the chief election official or designated person will investigate and determine if a security violation has occurred. If a security violation has occurred, and the election official or designated person has determined a security violation has occurred, the unit shall be taken out of service and all votes cast on the AccuVote-TSX unit will be manually tabulated.

9. Prior to inserting the memory card into the AccuVote-TSX unit to complete the programming of the unit for an election, the Ballot Station firmware will be reinstalled from a trusted version. That trusted version is may be provided by the California Secretary of State's office. This process is accomplished by placing a memory card with a trusted version of the software into the AccuVote-TSX while it is powered off and turning the unit on. To complete the instructions, follow procedures and the AccuVote-TSX on-screen instructions.

10. If prior to an election, there is a legitimate question about the secure chain of custody with respect to an install memory card or the Ballot Station firmware on an install memory card, the chief elections official or designated person will investigate and determine an appropriate course of action if a violation has occurred with respect to the secure chain of custody on the install memory card or the Ballot Station firmware on the install memory card. If the chief elections official or designated person has determined that a violation has occurred with respect to the secure chain-of-custody on the install memory card or the Ballot Station firmware on the install memory card, all AccuVote-TSX units programmed with the install card will be immediately taken out of service and any votes all ready cast on an AccuVote-TSX will be manually tabulated and reported from the AVPM paper audit trail. The Secretary of State will be notified of this event.

11. Each memory card shall be programmed in a secured facility under the supervision of the registrar of voters or registrar of voters' staff. The memory card(s) shall be inserted into the assigned AccuVote-TSX unit as soon as practicable and a serialized, tamper-evident seal shall be immediately applied to the AccuVote-TSX memory card door. The county may also choose to seal other areas of the AccuVote-TSX with tamper-evident seals for additional security. Once a memory card is programmed for the election, the chain-of-custody log shall be immediately updated upon insertion of the AccuVote-TSX memory card(s). The chain-of custody log shall be updated upon insertion of the memory card and have the AccuVote-TSX units' serial number and the memory card serial number logged into the chain-of-custody tracking sheet designed for that purpose.

12. The county shall maintain a chain-of-custody log that records which memory cards and which serialized tamper-evident seals is assigned to which AccuVote-TSX units. Any breach of control or break in the chain-of-custody log determined to have occurred prior to Election Day of the memory card and or AccuVote-TSX unit or tamper-proof seal shall require that a replacement memory card should be programmed and issued in the presence of two election officials or designated persons.

13. On Election Day, prior to any ballots being cast on any unit, the integrity of the tamper-evident seal(s) shall be verified by the precinct officer before opening the AccuVote-TSX. The serial number of the seal shall also be verified against the log provided to the precinct officer. This procedure shall be witnessed by at least one other precinct officer or staff of the registrar of voters.

14. If there is a discrepancy between the tamper evident seal log and the serial number(s), the discrepancy shall be confirmed by one or more of the remaining members of the precinct board, documented, and immediately reported to the county elections official for the jurisdiction. The elections official or designated official will investigate and determine the appropriate course of action. If a discrepancy is determined to have occurred, The AccuVote-TSX shall be taken out of service until the election official determines the appropriate course of action.

15. If being used to meet the accessibility provisions of federal or state law, or if for any reason only one such unit is being used at the precinct, the county will establish poll worker training procedures to mitigate one vote being cast on the AccuVote-TSX unit. The procedures should establish methods that can be used by poll workers to attempt to have at least two more ballots are cast on the machine, even if not by a voter needing its accessibility components, in order to protect the privacy of the voter.

16. The County will be responsible for procedures for maintaining a chain-of-custody log throughout the Election Day process, including return of the memory card to the election office or drop-off location. Security transport bags will be used during the transport phase of the memory card back to the drop off location or election office.

17. If, upon return of the sealed memory card in the AccuVote-TSX or sealed memory card transport bag, it is determined that a potential breach of the seal has occurred, the breach must be investigated by the appropriate elections

officials and appropriate steps should be taken as a result of those findings in the investigation. Reconciliation should also establish whether any discrepancies for total votes between the memory card and the AccuVote-TSX.

Security of AccuVote-OS units

The following are areas based on prior recommendations for improving security of the AccuVote-OS unit, and best practices for security of the AccuVote-OS unit:

- 1 Each memory card shall have a permanent serial number assigned to it.
- 2 The county shall maintain a written chain-of-custody log that accurately records the chain-of-custody of each memory card and AccuVote-OS unit from the point of programming the memory card for use in the election through the time of completion of the official canvass.
- 3 Each memory card shall be programmed in a secured facility under the supervision of the registrar of voters or registrar of voters' staff. The memory card(s) shall be inserted into the assigned AccuVote-OS unit as soon as practicable and a serialized, tamper-evident seal shall be immediately applied to the AccuVote-OS memory card security bar. The county may also choose to seal other areas of the AccuVote-OS with tamper-evident seals for additional security. Once a memory card is programmed for the election, the chain-of-custody log shall be immediately updated upon insertion of the AccuVote-OS memory card(s). The chain-of-custody log shall be updated upon insertion of the memory card and have the AccuVote-OS unit serial number and the memory card serial number logged into the chain-of-custody tracking sheet designed for that purpose.
- 4 The county shall maintain a chain-of-custody log that records which memory cards and which serialized tamper-evident seals is assigned to which AccuVote-OS units. Any breach of control or break in the chain-of-custody log prior to Election Day of the memory card and/or AccuVote-OS unit or tamper-proof seal shall require that the memory card shall be replaced in the presence of two election officials.
- 5 On Election Day, prior to any ballots being cast on any unit, the integrity of the tamper-evident seal(s) shall be verified by the precinct officer. The serial number of the seal shall also be verified against the log provided to the precinct officer. This procedure shall be witnessed by at least one other precinct officer or staff of the registrar of voters.
- 6 If it is detected that the tamper-evident seal has been broken prior to turning on the AccuVote-OS , or if there is a discrepancy between the log and the serial number, the discrepancy shall be confirmed by one or more of the remaining members of the precinct board, documented, and immediately reported to the county elections official for the jurisdiction. The unit shall be taken out of service until the election official investigates and determines the appropriate course of action.
- 7 The County will be responsible for procedures for maintaining a chain-of-custody log throughout the Election Day process, including return of the memory card to the election office or drop-off location. Security tamper evident seals will be used during the transport phase of the memory card back to the drop off location or election office.
- 8 If, upon return of the sealed memory card in the AccuVote-OS or sealed memory card transport bag, it is determined that a potential breach of the seal has occurred, the breach must be investigated by the appropriate elections officials and appropriate steps should be taken as a result of those findings in the investigation. Reconciliation should also establish whether any discrepancies between the memory card and the AccuVote-OS, as well as the summary reports occurred.
- 9 Any replacement seals shall be logged and verified using a log designed for that purpose,

10.2 Logical Security of System and Components

This section lists the system service components that should be implemented for the voting tabulation system. This includes services and ports, passwords, anti-virus protection, and other components. The procedures can be found in the Windows Configuration Guide and the Client Security Policy. There may be other requirements as needed:

10.2.1 Essential and non-essential services and ports

- All network services and network ports are to be turned off, except those explicitly required to run the GEMS software;
- the “auto run” feature in Windows is to be disabled;
- the boot order is to boot from the hard drive only;
- the BIOS is to be password protected to prevent changes to the boot order;
- The specifics for understanding and implementing these items can be obtained from Premier.

10.2.2 User-level security

GEMS Passwords

A minimum of two people in the county election office shall have usernames and passwords with administrative access to the GEMS election database (These may be different than the server administrators and are specific to the election). The GEMS passwords shall be at least 6 to 8 digits and include a combination of alpha and numeric characters.

Passwords shall be changed before each election. Each user should immediately change the password, if the password is suspected of being disclosed, or is known to have been disclosed, to an unauthorized party.

Users are responsible for all activities performed with their personal login-IDs. Login-IDs may not be utilized by anyone but the individuals to whom the logons have been issued. Users shall not allow others to perform any activity with their login-IDs. The GEMS server, workstation, or terminal should not be left unattended without first logging-out or invoking a password-protected screen saver, as is practicable with security procedures and best practices for administering elections.

10.2.3 Anti-Virus protection

An anti-virus program may be installed on the GEMS server. Premier recommends the MacAfee virus scan. The virus program shall be updated and a virus scan run immediately prior to each election. The current and updated dat files should be downloaded on another system, virus checked and then installed and verified.

10.2.4 Procedures for verifying, checking, and installing essential updates and changes

Software to be loaded to the server should be virus scanned and also verified to come from an authorized source. The software may be provided by the California Secretary of State’s Office. Once verified, the software should be installed and retested to verify the software is correctly functioning.

10.2.4.1 Audit records for the changes showing what, when, who, and why

A log of the server should be kept to track what is on the server and what is installed by whom and when. This should be done by a minimum of 2 people and the log signed by each individual.

10.2.4.2 Installation procedures

Updates should be received via CD through the mail or downloaded on a secure system and then virus scanned and transferred to the GEMS server once validated.

Software to be loaded to the server should be virus scanned and also verified to come from an authorized source. The software may be provided by the California Secretary of State's Office. Once verified, the software should be installed and retested to verify the software is correctly functioning.

10.2.4.3 Acceptance testing after the installation.

Verify that all of the expected functionality of the GEMS workstation is available. Mark each function on a signoff sheet, once it has been verified. The following functions are to be verified:

1. Copy from CD
2. Restore database
3. GEMS version
4. Reports version
5. View card in Card Editor
6. Print ballot artwork
7. Print administrative reports
8. Record/play back audio
9. Download memory card
10. Upload memory card
11. Print results report
12. Perform a backup
13. View GEMS User's Guide
14. Verify GEMS "Read Me" file
15. JResult Client version

10.3 Security Procedures for Central Processing

The following are some best practices for ensuring the security of the central ballot processing system:

- a. Ballots processed at the central location shall be secured from tampering, theft and damage in the same way that official ballots are secured.
- b. Appropriate physical, technical and administrative processes and procedures shall be in place to ensure security of the central processing system.
- c. Voting units utilized for early voting shall be secured at the end of each day and appropriate security logs shall be kept.
- d. Election material used on a daily basis (e.g., voter access cards, VCProgrammer, AccuVote-OS and AccuVote-TSX units, Supervisor and Administrator cards and, official ballots) shall also be secured when not in use.
- e. The server shall be secured and locked when not in use and only used by authorized personnel. This includes the voting equipment connected to the server.

Security of Votes

Tampering, Theft, Alteration — The elections official shall ensure the security of all votes cast are free from tampering, theft, or alteration, and shall ensure that the results of votes counted exactly reflects the number of voters and the voter's selections.

Voting on Multiple Days — If early voting takes place on more than one day, the elections official shall establish procedures to reconcile each day's voting activity and to ensure that votes and other activities have been recorded and securely stored. The number of votes cast each day shall be compared to the number of voters who appeared requesting to vote and who were authorized to vote, as determined by the roster, or by other means.

Voted Ballots Returned to Elections Office — Voted ballots from each day's voting shall be returned to the elections office, and an audit trail produced and preserved documenting the results from each day's voting.

Storage at Election Warehouse

If the memory cards is to be installed in the voting terminals prior to distribution to the vote centers, the voting terminals should be kept in a secure location after the memory card installation. The location should restrict access to only authorized personnel. Logs shall be kept to track the memory card installation.

Secure Storage — Voting devices shall be securely stored when not in use. Storage should be in a locked location, with access to that location authorized by an election official or designee.

10.4 Security Procedures for Polling Place

The following are some best practices for ensuring the security of the precinct ballot processing system:

Storage at Vote Center

After distribution of the AccuVote-OS and AccuVote-TSX units to the vote centers, the units should be kept in a secure location at the vote centers. The location should restrict access to only authorized personnel. If possible, appropriate to protecting the security of the voting location, tamper-evident seals and other security mechanisms should be placed on entries into the secure location.

The AccuVote-OS and AccuVote-TSX units shall be inventoried, sealed and verified. Any discrepancies should be noted and rectified prior to opening and setup on Election Day. The discrepancies should be immediately reported to the authorized election official or designee.

Election supplies, such as, rosters, official ballots, signs, shall be kept in the possession of the designated election official and verified and inventoried according to established procedures.

10.5 Audit Trails

All system audit logs for software and hardware should be retained as part of the official elections record. The Logic and Accuracy test results as well as maintenance and repair logs should also be maintained. This should include the audit logs for the precinct equipment used for an election.

10.6 Audit Logs – AccuVote OS

10.6.1 Archiving the OS Audit Report to Soft Media

This procedure allows memory card data to be uploaded to HyperTerminal, captured, stored on write-once media and retained. It is followed by an optional procedure to print the audit logs. Office of the Secretary of State procedures require that the audit logs be archived to soft media. Printing is not required.

- Connect the AVOS unit to the host computer via the same cable you would normally use for download and upload.
- Open HyperTerminal on the host computer. At the *New Connection* screen enter a name for the connection and press OK.
- On the *Connect To* screen select the COM port active in AVOS communications. (Commonly COM1)
- Communication Properties settings are:
9600 Bits per Second

8 Data Bits

None Parity

1 Stop Bits

Hardware Flow Control

- The HyperTerminal connection is now active with the AVOS unit. Select the Transfer>Capture Text tool from the menu bar. Select the path and filename where the memory card data will be captured. (example capture.txt)

- Turn on the AVOS unit in Diagnostic Mode by pressing YES and NO at the same time and follow the screen prompts.

SET SYSTEM CLOCK? (Press NO)

DUMP MEMORY

CARD IMAGE (Press YES)

SEND RESULTS

BY TELEPHONE? (Press NO)

SEND RESULTS

BY DIRECT MODE? (Press YES)

USE XMODEM PROTOCOL? (Press NO)

DUMPING MEMORY

CARD XXXX (No interaction)

The AccuVote-OS now begins transmission of the memory card immediately and the operator will see the bytes counting down on the AVOS LCD.

MC IMAGE SENT

Once the transfer has completed Select STOP from the Transfer>Capture Text menu in HyperTerminal. The memory card data is in the captured file.

SEND ANOTHER? (Yes or No)

If additional memory card images are to be transmitted from more than one memory card, press Yes, remove the uploaded card, then insert the next card to upload. Repeat the HyperTerminal Capture Text process with a different file name for each memory card. If no other cards are to be uploaded, press NO.

- Use any off-the-shelf media burning software on the host computer to archive the captured memory card data file to write-once media.

10.6.2 Printing the Audit Logs

The AccuVote-OS Audit report may be printed in Pre-Election and Post-Election Modes. A Memory Card label precedes the Audit Report, identifying the polling place and the election held.

The Audit report includes:

- Time
- Date
- Election status
- Pre-election statistics
- Election statistics
- Overrides
- Post-election statistics
- Reports printed
- Transaction log.

10.6.3 Election status

The election statuses are 0 through 6:

0 Memory Card is initialized

1 Memory Card is programmed

2 election is in progress

3 AccuVote-OS Ender card has been read but Election Results report has not finished printing

4 Memory Card is in Post-Election Mode but election results have not yet been transmitted to the host computer

5 Memory Card is in Post-Election Mode and election results have been transmitted to the host computer

6 Memory Card is in Post-Election Mode, election results have been transmitted to the host computer and Audit report has been printed

10.6.4 Pre-election statistics

The following items are listed on the Audit report in the **Pre-Election** section:

Ballot Tests

The total number of ballot card tests performed in Pre-Election Mode.

Test Uploads

The total number of times ballot card test results are uploaded.

10.6.5 Election statistics

The following fields are printed in the **Election** section of the Audit report.

Times Restarted

The number of times the election process has been restarted. Restarts occur when either the power switch on the AccuVote-OS unit is turned off, the AccuVote-OS unit experiences a power failure or the Memory Card is removed and re-inserted in the same or another AccuVote-OS.

Non-Abs Ballots

The number of non-absentee ballots counted.

Absentee Ballots

The number of absentee ballots counted.

Total Ballots

The total number of ballots counted. This number should be equal to the sum of # Non-Abs Ballots and # Absentee Ballots.

10.6.6 Overrides

This section includes the number of overrides printed for each of the following:

- Overvoted race
- Unvoted race
- Undervoted race
- Unvoted card
- Straight party overvote
- Multi-party vote
- Duplicate candidate vote
- Oversize marks
- Total number of ballot card overrides.

10.6.7 Reports Printed

The following fields are printed in the **Reports printed** section of the Audit report.

Download Zero

The number of Zero Total reports printed after programming the voting center to a Memory Card.

Election Zero

The number of Election Zero reports printed, prior to counting ballots in Election Mode.

Election Results

The number of Election Results reports printed after the election has been completed, both after electronically locking the AccuVote-OS and in Post-Election Mode.

Test Zero

The number of Zero Total reports printed prior to counting test ballots in Pre-Election Mode.

Test Results

The number of Test Results reports printed in Pre-Election Mode.

Audit Reports

The total number of Audit Reports printed.

10.6.8 Transaction Log

The Transaction Log lists each transaction carried out on the Memory Card in chronological order as well as any errors that have occurred. Up to 30 different comments may be listed. The log lists the time each transaction was made, the date the card was initialized and the date when each session was started.

Descriptions are provided for the following fields in the Transaction Log. All other fields printed in the log should be self-explanatory.

Absentee Count

An **Absentee Count card** has been processed in Election Mode.

Bal Count End

An **AccuVote-OS Ender card** has been processed in Election Mode.

Bal Count Start

The first ballot is counted in Election Mode.

Bal Test Start

The first ballot is counted in Pre-Election Mode.

Clear Counters

This transaction is logged after a Memory Card has completed programming, before counting test ballots in Pre-Election Mode and before counting ballots in Election Mode.

Com Error

A communications error between the AccuVote-OS unit and the Vote Tally System has occurred.

Download End

Memory Card programming has completed.

Download Start

Memory Card programming has begun.

Duplicate Card

A Memory Card copy has been made.

Ender Card

An AccuVote-OS Ender card has been read.

Host Error

Memory Card programming or election results transmission has been interrupted by an action taken by GEMS.

Mem Card Reset

The Memory Card has been reset to Pre-Election Mode.

Prep for Elect

The Memory Card has been set to Election Mode.

Session Start

The unit has been turned on and/or the Memory Card has been installed.

Unknown Trans

A transaction has occurred which the unit does not recognize.

Unvoted Bal Test

The first ballot is counted in the Unvoted Ballot Test.

Upload Error

An error occurred in the course of transmitting election results to the host computer.

Upload Start

Transmission of election results to the host computer has begun.

Voted Bal Test

The first ballot is counted in the Fully Voted Ballot Test.

10.6.9 Resetting the Memory Card to Pre-Election Mode

USE CAUTION WHEN RESETTING A MEMORY CARD. AUDIT INFORMATION MAY BE LOST IF PROCEDURES ARE NOT FOLLOWED.

A Memory Card may be reset to Pre-Election Mode in Supervisor Functions either in Election Mode or Post-Election Mode. *Note that all election results are lost when a Memory Card is reset to Pre-Election Mode and may not be recovered.*

The prompts displayed when resetting a Memory Card to Pre-Election Mode differ according to whether a Memory Card has been audited. A Memory Card may be audited in Post-Election Mode after election results are transmitted to the host computer.

Resetting After Auditing the Memory Card

NOTE: Do not reset a Memory Card until you have audited it. If the prompt “CARD NOT AUDITED RESET?” appears, Press NO. Audit the Memory Card, then restart the process to reset the card

To reset an audited Memory Card to Pre-Election Mode, press YES in response to

RESET CARD TO
PRE-ELECTION?

The Memory Card is automatically reset to Pre-Election Mode, after which

REMOVE RESET

MEMORY CARD

is displayed. Remove the reset Memory Card from the AccuVote-OS.

10.6.10 Clearing the Memory Card

Clearing a Memory Card causes all programmed election information and results to be removed from a Memory Card. ***It is not possible to recover any of the information once the Memory Card has been cleared.*** Clearing a Memory Card also causes any information defined to the Memory Card in Setup Mode to be lost.

The prompts used to clear a Memory Card in Pre-Election Mode are different from those in Election and Post-Election Modes. Furthermore, the prompts displayed in Election and Post-Election Modes differ according to whether a Memory Card has been audited.

Memory Cards must be cleared to be reused in future elections.

10.6.10.1 Pre-Election Mode

[NOTE: Do not clear a Memory Card until you have audited it. If the prompt "CARD NOT AUDITED CLEAR?" appears, Press NO. Audit the Memory Card, then restart the process to clear the card](#)

1 Press YES in response to

CLEAR THIS
MEMORY CARD?

2

CARD PROGRAMMED
CLEAR?

is displayed—press YES.

3

CLEARING
MEMORY CARD

and

REMOVE CLEARED
MEMORY CARD

are shown. Remove the blank Memory Card and remove any attached label.

10.6.10.2 Election and Post-Election Modes

NOTE: Do not clear a Memory Card until you have audited it. If the prompt “CARD NOT AUDITED CLEAR?” appears, Press NO. Audit the Memory Card, then restart the process to clear the card

The following prompts are displayed when clearing a Memory Card audited after transmitting election results to the host computer in Election or Post-Election Modes.

1 Press YES in response to

CLEAR THIS
MEMORY CARD?

2 Then

CARD AUDITED
CLEAR?

is displayed—press YES.

3 Finally,

CLEARING
MEMORY CARD

and

REMOVE CLEARED
MEMORY CARD

are displayed. Remove the blank Memory Card and remove any attached label.

10.7 TSx Audit Logs

IMPORTANT: See Appendix A and sections 10.8.2.6 through 10.8.2.10 for additional information regarding TSx log retrieval and management.

10.8 Audit Logs Available from GEMS, and Assembling an Election Audit Materials Archive

Once the election has finished, audit logs are printed, election results certified, official election results reports printed, and any other election materials archived as required. The election is declared closed.

10.8.1 Audit and archive [materials](#)
[Materials for](#) the audit and archive phase of the election include:

1. Audit and archive procedures
2. AccuVote-TS memory cards

3. AccuVote-OS memory cards
4. AccuVote-OS voted ballots
5. AccuVote-TS reports
6. AccuVote-OS reports
7. GEMS final election results reports
8. Results import files
9. Results export files
10. Database backups
11. Administrative reports
12. AccuVote-OS test ballots
13. Database import files
14. Election Media Processors
15. VCProgrammer

NOTE: Not all of the items in the above list may have been utilized in the election to be audited and archived. [The available materials arising from the election and included in the list above comprise the election archive package.](#)

10.8.2 Audit and archive materials and procedures

Audit and archive materials shall include all materials assembled according to the following procedures. All ballot materials, such as AccuVote-OS ballots, AVPM canisters, and memory cards shall be archived in secure, climate controlled facilities, and kept away from light. Use the list below (and the retrieval procedures) to complete the package of audit materials.

10.8.2.1 AccuVote-OS Audit reports

The election archive shall include all AccuVote-OS Audit log reports.

1. Connect an AccuVote-OS unit to AC power and power on
2. Assemble all voted AccuVote-OS memory cards
3. For each AccuVote-OS memory card:
 - a. Print the Audit Report
 - b. Once the report is printed, detach and file the report as part of the election archive, after any audit is complete
 - c. Remove the memory card

10.8.2.2 AccuVote-OS memory cards

Assemble all AccuVote-OS memory cards used in the election.

10.8.2.3. AccuVote-OS reports

The election archive [shall](#) include all AccuVote-OS Zero and Election Totals reports. Assemble all:

1. Final test AccuVote-OS Zero and Election Totals reports
2. AccuVote-OS Logic and Accuracy Test Zero and Election Totals reports
3. Official AccuVote-OS Zero and Election Totals reports

10.8.2.4 AccuVote-OS test ballots

The election archive shall include all AccuVote-OS test ballots. AccuVote-OS test ballots should be assembled as

follows:

1. Every AccuVote-OS card/precinct identifier/language ballot proof combination, bearing authorizing signatures and time/date stamps
2. All AccuVote-OS card/precinct identifier/language combination test ballots
3. Every AccuVote-OS card/precinct identifier/language combination Logic and Accuracy Test deck

10.8.2.5 AccuVote-OS voted official ballots

The election archive shall include all AccuVote-OS ballots. Assemble all voted AccuVote-OS ballots, sorted by memory card (vote center/machine ID).

10.8.2.6 AccuVote-TS Accumulator log

All AccuVote-TS Accumulator Audit logs shall be printed and archived.

1. Assemble all AccuVote-TS units used for results accumulation (installed with original memory cards with voted ballots)
2. For each AccuVote-TS Accumulator unit:
 - a. Connect the AccuVote-TS unit to AC power, and power on
 - b. Launch the Accumulator
 - c. In the Accumulator, launch the Accumulator Audit log
 - d. Print the Accumulator Audit log
 - e. Close the Accumulator

10.8.2.7 AccuVote-TS Audit reports

The election archive shall include all AccuVote-TS Audit reports in soft copy.

IMPORTANT: See Appendix A for procedures to prepare soft copies of AccuVote-TS Audit Logs and Election Information. The Office of the Secretary of State requires the audit logs be stored in soft copy. Making a printed copy as described in Appendix A is optional.

10.8.2.8 AccuVote-TS ballot images

The election archive should include all AccuVote-TS ballots images, printed and archived from GEMS. These images are captured in the View Ballot Votes window.

1. Launch the View Ballot Votes window
2. For every vote center/machine combination listed in the display panel at the top of the View Ballot Votes window:
 - a. Click on the Print All button
 - b. Once all ballots on the memory card have been printed, file the ballots
3. Close the View Ballot Votes window

10.8.2.9 AccuVote-TS memory cards

If an AccuVote-TS memory card contains any official election data including but not limited to votes, error messages and log entries, the contents must be backed up and kept on file for 22 months. Once a TS memory card has been backed-up and archived, that card may be cleared.

10.8.2.10 AccuVote-TS reports

The election archive should include all AccuVote-TS reports. Assemble all:

1. Final test AccuVote-TS Zero and Election Totals reports
2. AccuVote-TS Logic and Accuracy Test Zero and Election Totals reports
3. Official AccuVote-TS Zero and Election Totals reports

10.8.2.11 Administrative reports

All administrative reports used in verification procedures should be assembled by election phase and included in the election archive. Reports should bear the signatures of the election administrator, as well as any other authorizing officials.

10.8.2.12 AVPM ballot record canisters

All AccuView Printer Module ballot record canisters consumed in the election shall be archived. Canisters should be removed from AccuVote-TS AccuView Printer Module units, then packaged and sealed to fulfill this task.

10.8.2.13 AVServer console log

The election archive shall include the AVServer console log.

1. In GEMS, click on the AVServer icon in the toolbar
2. Click on the Log tab in the AVServer console
3. Click on the Print button
4. Once the log has printed, click on the Close button in the console
5. File the AVServer log

10.8.3 Database backups

Include all database backups performed in the course of the election in the election archive, ensuring that each backup is labeled with the election phase as well as the date and time the backup was performed. Ensure that each copy of the election directory that was created in the course of the election is included with the archive data.

In order to back up a database:

1. In GEMS, click on Election in the menu bar, then Backup in the drop-down menu
2. In the Save As window, set the folder location to the appropriate folder location on the GEMS server hard disk
3. Assign the correct backup name in the File name field, and click on the Save button
4. Copy the election's <EID> folder to the CD-R disk. The path to this folder is C:\Documents and Settings\All Users\Application Data\Premier Election Solutions\GEMS 1.21\Data\<EID>.
5. Once the backup has been created, copy the database backup file to a new CD-R
6. Remove external media with the database backup, and file

10.8.4 Election Media Processor

Include all logs from each Election Media Processor used in the election:

1. In the Election Media Processor software user interface, click on the Logs button
2. Click on the Download Log button
3. Click on the Print button to print the log
4. Once the Download Log has completed printing, click on the Upload Log button
5. Click on the Print button to print the log
6. Once the Upload Log has completed printing, click on the Error Log button
7. Click on the Print button to print the log

10.8.5 Event Viewer log

Following election close, operating system event logs shall be archived from every Premier Election Solutions election workstation, including the GEMS server and PCS workstations. Refer to the *GEMS System Administrator's Guide section 3.46* and the *PCS User's Guide* for a procedure to print these logs.

10.8.6 GEMS Audit log

The election archive shall include the GEMS Audit Log. The GEMS Audit log contains a complete record of all transactions that have occurred in the election, ordered by date and time.

1. In GEMS, select GEMS in the menu bar, then Audit Log in the drop-down menu
2. In the Audit Log window, click on the Print button to print the Audit log
3. Configure print parameters in the Print window as necessary, then click on the OK button
4. Once the Audit Log has been printed, click on the OK button in order to close the Audit Log window

10.8.7 GEMS final election results reports

The election archive shall include all GEMS Election Summary, SOVC, and Cards Cast reports printed. GEMS election results reports should be assembled and archived **from the following election phases:**

1. Transmission configuration and testing
2. AV OS Central Scan configuration and testing
3. Regional processing
4. Pre-Election Logic and Accuracy Testing
5. Election close (Zero Election Summary report)
6. Polling results only
7. Early voting results only
8. Absentee results only
9. Imported results only
10. Write-in candidate tallies
11. Provisional results
12. Post-Election Logic and Accuracy Testing
13. Recount
14. Final

10.8.8 Import files

Include any electronic files imported into the GEMS database in the election archive, including jurisdictional definition and race/candidate information. These files may include the:

- StandardImportfile
- LAImportfiles
- ImportVRegfile
- ImportRichTextfile
- Audioimportfiles

10.8.9. Poster log

Poster logs should be added to the election archive.

1. In GEMS, click on Servers in the menu bar, then Poster in the drop-down menu
2. Select the desired filter options for the log

3. In the Poster window, click on the Print button

4. Once the log has printed, click on the Close button in the console

10.8.10 Regional Server log

If regional processing was employed in the election, include the Regional Server log in the election archive. On the GEMS server at election central:

1. Select Servers in the menu bar, then Regional Server in the drop-down menu
2. Click on the Log tab in the Regional Server console
3. Click on the Print button
4. Once the log has printed, click on Close

On each of the regional client computers:

1. Click on GEMS in the menu bar, followed by Send Regional Results in the drop-down menu
2. Click on the Log tab in the Send Regional Results console
3. Click on the Print button
4. Once the log has printed, click on Close

File the Regional Server and Send Regional Results logs.

10.8.11 Results export files

Any election results export files generated from the GEMS database should be included in the election archive.

10.8.12 Results import files

If election results counted using non-Premier Election Solutions voting devices were introduced into the GEMS database, these files should also be archived.

10.8.13. VCProgrammer audit file

If VCProgrammer was used in the election, include application's audit file in the election's archives.

VCProgrammer's audit file is named 'VCPLog.txt'. This file is saved in C:\Documents and Settings\\Application Data\Premier Election Solutions\VCProgrammer 4.7

1. Copy the 'VCPLog.txt' file generated by each instance of VCProgrammer used in the election onto external archive media.
2. Remove the external media containing the audit logs, and file.

List of Reference / User Manuals

The following is a list of reference / user manuals related to the Premier AccuVote® system:

1. AccuFeed_1.0_Hardware_Guide
2. AccuView_Printer®_Module_Hardware_Guide
3. AccuVote®-OS_Central_Count_2.00_Users_Guide
4. AccuVote®-TSX_Hardware_Guide
5. AccuVote®-TSX_Pollworkers_Guide
6. AVPM_Service_Guide_Revision
7. AVPM_Single_Roll_Opening_and_Closing_Procedures
8. GEMS®_1.18_Election_Administrators_Guide
9. GEMS®_1.18_Product_Overview_Guide
10. GEMS®_1.18_Reference_Guide
11. GEMS®_1.18_System_Administrators_Guide
12. GEMS®_1.18_Users_Guide
13. Key_Card_Tool_4.6_Users_Guide
14. VCProgrammer_4.6_Users_Guide
15. Voter_Card_Encoder_Users_Guide
16. Ballot_Station_4.6_Users_Guide
17. AccuVote®-OS_Precinct_Count_1.96_Users_Guide
18. AccuVote®-OS_Pollworkers_Guide

System Administration

Premier's Windows Configuration Guide



Revision 1.0
September 17, 2007

Copyright

Premier's Windows Configuration Guide

© Premier Election Solutions ULC, 2006, 2007.

All Rights Reserved

Important Notice

This document is the copyrighted property of Premier Election Solutions. Any reproduction, distribution, display, translation, or modification of any portion of this document without the express written authorization of Premier Election Solutions is prohibited. Additional copies may be purchased from Premier Election Solutions for a fee.

Premier Election Solutions ULC
1200 W. 73rd Street, Suite 350
Vancouver, B.C.
Canada V6P 3G5

Disclaimer

The information in this document is provided 'as is' and without warranty. Premier Election Solutions will not be liable for any incidental, consequential, or other damages of any type or nature, resulting from the provision or use of the information contained herein. All information is subject to change at any time without notice. Users of this document assume sole responsibility for their use of the information contained herein, as well as any products, software, or other materials that may be provided by Premier Election Solutions. Care should be exercised by such users to assure compliance with all applicable laws, rules, and regulations.

Trademarks

ASSURE™, AccuVote®, AccuView Printer®, BallotStation®, Central Tally System™, ExpressPoll®, GEMS®, Key Card Tool™, Optical Scan Accumulator Adapter™, UAID™, and VCProgrammer™ are trademarks owned by or licensed to Premier Election Solutions. All other trademarks are the exclusive property of their respective owners.

Part number: 744-5034

Document History

Document Number	Date	Remarks
DETS00000A	September 17, 2007	Initial document created.

Table of Contents

1.	Introduction	1-1
1.1.	Scope	1-1
1.2.	Audience	1-1
2.	Securing Windows Machines	2-1
2.1.	Overview.....	2-1
2.2.	Hardware	2-1
3.	Windows Components.....	3-1
3.1.	Basic components	3-1
3.2.	Additional security components	3-1
4.	Update Packages	4-1
4.1.	Windows Server 2003 R2 Standard specifications	4-1
4.2.	Windows XP Professional specifications	4-1
4.3.	Windows 2000 Server SP4 specifications.....	4-2
5.	Services to Enable.....	5-1
6.	Windows System Settings	6-1
6.1.	Data Execution Protection (DEP).....	6-1
7.	Security Policies	7-1
8.	File Permissions	8-1
9.	Registry Permissions.....	9-1

1. Introduction

1.1. Scope

This document describes the Microsoft Windows® configuration that is recommended by Premier Election Solutions for use with Premier's election products, including the Global Election Management System (GEMS).

Note: The configuration information in this document is provided as reference. The configuration of individual systems may have slight variations.

1.2. Audience

This document is intended for Premier Election Solutions' staff responsible for building, verifying, and shipping servers to clients. It may also be used as a reference by qualified, customer IT personnel to construct their own servers for use with Premier's election products.

Note: The specifications outlined in this document are subject to change. For example, Premier Election Solutions may recommend the installation of new Windows Update packages on servers defined for use with our products. Before configuring a system for a client, verify with your Premier Election Solutions service manager that you are using the latest information.

2. Securing Windows Machines

2.1. Overview

Securing a Windows computer is an ongoing process. It is the responsibility of the jurisdiction using the equipment to follow all local rules and laws with respect to ensuring that their system is as secure as possible. For a description of additional security considerations we strongly recommend that the operators of the system review *Premier's Client Security Policy* document.

Premier will continue to review the security and configuration settings outlined in this document and will, from time to time, release addendums or updates to this document.

Note that this document does not describe how to install the Microsoft Windows operating system. This information is provided by Microsoft.

2.2. Hardware

There are a number of steps outside the configuring of Windows that need to be performed to ensure that the machines remain secure. They are:

- Keep the machines in a secure, locked room and only allow access to authorized operators.
- Ensure there is a password on the BIOS Setup.
- Only allow the system to boot from the hard drive (Note: The system should be booted only after Windows is installed and configured correctly).

3. Windows Components

3.1. Basic components

The following windows components should be installed:

- Internet Explorer Enhanced Security Configuration
- Update Root Certificates
- Dynamic Host Configuration Protocol – Only if the machine is going to provide DHCP services for the network.

No other components are required.

To install these components, use “Control Panel->Add Remove Programs->Add/Remove Windows Components”.

If you are using GEMS 2.0 and SQL Server, install this software before proceeding. See the Microsoft SQL Server documentation for SQL Server installation and configuration instructions. See the *GEMS 2.1 System Administrator's Guide* for GEMS installation instructions.

3.2. Additional security components

Additional security components must be installed for Windows XP and 2003. The required files are included in a zip file with Microsoft's Threats and Countermeasures Guide.doc. To find and this zip file and install the required files:

- 1) Download Microsoft's *The Threats and Countermeasures Guide* .zip from Microsoft's web site.

To locate these files, go to: <http://www.microsoft.com> and search for: "The Threats and Countermeasures Guide".

This zip file can also be located at:

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=1b6acf93-147a-4481-9346-f93a4081eea8>.

- 2) Unzip the contents of the Threats_and_Countermeasures_Guide.zip file into a temporary directory.
- 3) Double-click on the “Threats and Countermeasures Guide Tools and Templates.msi” file in the temporary directory.
- 4) Double-click on the “Update_SCE_with_MSS_Regkeys.vbs” file to install the additional security policies.

These policies are documented in Chapter 10 of The *Threats and Countermeasure Guide* document.

For a description of these files, see section 7, *Security Policies* in this document.

4. Update Packages

4.1. Windows Server 2003 R2 Standard specifications

The server should have the following packages installed:

- Internet Explorer 7
 - Security Update for Internet Explorer 7 KB928090
- Security Update for Windows Server 2003
 - KB896424, 896428, 899587, 899588, 899589, 899591, 901017, 901214, 902400, 893756, 896358, 905414, 908519, 911562, 911927, 912919, 914388, 917422, 904706, 917953, 918118, 918439, 920213, 920670, 920683, 920685, 921883, 922819, 923191, 923414, 923689, 923694, 923980, 924191, 926436, 928090, 928255, 928843, 917734, 914389, 931768, 932168, 931784, 930178, 925902
- Update for Windows Server 2003
 - KB898715, 908531, 910437, 911280, 911897, 904942, 922582, 931836
- Security Update for Windows Media Player 6.4
 - KB925398
- Malicious Software Removal Tool
 - KB890830

4.2. Windows XP Professional specifications

The server should have the following packages installed:

- Microsoft Windows Installer 3.1
- Internet Explorer 7
- Security Update for Windows XP
 - KB913433, KB890046, KB893756, KB896358, KB896422, KB896423, KB896424, KB896428, KB899587, KB899589, KB899591, KB901017, KB901214, KB902400, KB904706, KB905414, KB905749, KB908519, KB911562, KB911567, KB911927, KB912812, KB912919, KB913580, KB914389, KB916281, KB917344, KB917953, KB918439, KB900725, KB929969, KB923980, KB926255, KB923689, KB920213, KB924270, KB923414, KB924496, KB923191, KB924191, KB922819, KB919007, KB920685, KB920670, KB920683, KB921398, KB922616, KB917422, KB914388, KB918118, KB927779, KB924667, KB927802, KB928843, KB928255, KB926436, KB932168, KB931261, KB930178, KB931784, KB925902
- Update for Windows XP
 - KB898461, KB900485, KB894391, KB908531, KB910437, KB911280, KB922582, KB916595, KB920872, KB930916, KB931836
- Windows XP Hotfix
 - KB839210, KB886185, KB887472, KB887742, KB888113, KB888302, KB890859, KB891781, KB885836, KB885835
- Security Update for Windows Media Player KB911564
- Security Update for Windows Media Player 9 KB917734

- Windows Genuine Advantage Validation Tool KB892130
- Windows Genuine Advantage Notification KB905474
- Malicious Software Removal Tool for January 2007 KB890830
- Cumulative Security Update for Internet Explorer for Windows XP KB925454, KB931768
- Cumulative Security Update for Outlook Express for Windows XP KB923694
- Security Update for Media Player 6.4 KB925398
- Security Update for Flash Player KB923789

4.3. Windows 2000 Server SP4 specifications

- Service Pack 4
- Since Windows 2000 Server has reached its end-of-life, all available high-priority updates should be applied to this product. No further updates will ever be released.

5. Services to Enable

The following table lists the services that should be running. All other services should be disabled. Note that any installed hardware specific monitoring services and anti-virus services should be set to automatic or manual rather than be disabled.

Use the Services editor (Control Panel->Administrative Tools->Services) to configure these services.

Service Name	Windows Version			Mode	Comment
	2000	2003	XP		
Application Management	x	x	x	Man.	Required to allow programs to be installed
COM+ Event System	x	x	x	Auto	
Computer Browser	x	x	x	Auto	
Cryptographic Services		x	x	Auto	
DCOM Server Process Launcher		x	x	Auto	
DHCP Client	x	x	x	Auto	Required if machine is using DHCP rather than static IP
DHCP Server	x	x		Auto	Required if machine is the DHCP Server for the network.
DNS Client	x	x	x	Auto	
DNS Server	x	x		Auto	Required if machine is the DNS Server for the network.
Event Log	x	x	x	Auto	
Logical Disk Manager	x	x	x	Auto	
Logical Disk Manager Administrative Service	x	x	x	Man.	
MSSQLSERVER	x	x	x	Auto	GEMS 2 - Required on SQL Server Machine
Network Connections	x	x	x	Man.	
Plug and Play	x	x	x	Auto	
Print Spooler	x	x	x	Auto	
Protected Storage	x	x	x	Auto	
Remote Access Connection Manager	x	x	x	Man.	Require if using RAS for dial-in connections
Routing and Remote Access	x	x	x	Man.	Require if using RAS for dial-in connections
Remote Procedure Call (RPC)	x	x	x	Auto	
Security Accounts Manager	x	x	x	Auto	
Server	x	x	x	Auto	
SQL Server (SQLEXPRESS)	x	x	x	Auto	GEMS 2- Required if not using SQL Server
SQL Server Browser	x	x	x	Auto	GEMS 2 - Required if want to shared databases with other machine
System Event Notification	x	x	x	Auto	
Telephony	x	x	x	Man.	Require if using RAS for dial-in connections
Windows Audio		x	x	Auto	

Windows Installer	x	x	x	Man.	
Windows Management Instrumentation	x	x	x	Auto	
Windows Management Instrumentation Driver Framework	x	x		Man.	
Windows Time	x	x	x	Man.	
Workstation	x	x	x	Auto	

If McAfee anti-virus software is installed the following services must be enabled:

McAfee Framework Services	x	x	x	Auto	Required for McAfee Anti-Virus Software
Network Associates McShield	x	x	x	Auto	Required for McAfee Anti-Virus Software
Network Associates Task Manager	x	x	x	Auto	Required for McAfee Anti-Virus Software

6. Windows System Settings

The following system-wide setting should be changed:

6.1. Data Execution Protection (DEP)

This setting applies to Windows XP and Windows Server 2003 only.

This system setting should be enabled for all programs, not just essential Windows programs and services. To enable DEP, select Control Panel->System->Advanced->Performance Settings->Data Execution Prevention and then select "Turn on DEP for all programs and services..."

7. Security Policies

Using the Local Security Policy editor (Control Panel->Administrative Tools->Local Security Policy), the following security policies should be set:

- Password Policy
 - Enforce password history: 24 – this will keep a history of 24 passwords, preventing them from being re-used.
 - Maximum password age: 45 days
 - Minimum password age: 1 day
 - Minimum password length: at least 8 characters
 - Password must meet complexity requirement: Enabled
 - Store Passwords using reversible encryption for all users in the domain: Disabled
- Account Lockout Policy
 - Account lockout duration: 5 minutes
 - Account lockout threshold: 5 Tries
 - Reset account lockout counter after: This should be set to a reasonable time value, such as 5 minutes. This controls how much time may elapse between failed login attempts before resetting the threshold counter.
- Audit Policy
 - Audit account logon events: Log Success and Failure
 - Audit account management: Log Success and Failure
 - Audit directory service access: Log Success and Failure
 - Audit logon events: Log Success and Failure
 - Audit object access: Log Success and Failure
 - Audit policy change: Log Success and Failure
 - Audit privilege use: Log Failure
 - Audit process tracking: No auditing – this would fill the audit with useless information
 - Audit system events: Log Success and Failure
- User Rights Assignment
 - Access this computer from the network: Remove all groups and users listed and add “Authenticated Users”.
 - Allow logon through Terminal Services: Remove all groups and users.
 - Back up files and directories: Only allow “Administrators” and “Backup Operators” groups.
 - Change the system time: Only allow “Administrators”
 - Debug programs: Remove all groups and users.
 - Deny access to this computer from the network: Add the “Users” group.
NOTE: If using RAS do not add “Users” to the list.
 - Deny logon as a batch job: Add the “Everyone” group.

- Deny logon through terminal services: Add the “Everyone” group.
 - Impersonate a client after authentication: Removal all groups and users except “Administrators” and “SERVICE”.
 - Log on as a batch Job: Remove all users and groups.
 - Log On locally: Removal all groups and users except for the “Users” and “Administrators” group.
 - Shut down the system: Remove all groups and users except for “Administrators”.
 - Restore files and directories: Only allow “Administrators” and “Backup Operators” groups.
- Security Options
 - Accounts: Rename administrator account: Rename to ‘localadmin’ as per Microsoft recommendation and by the Centre For Internet Security’s scoring tool.
 - Accounts: Rename guest account – Renamed to ‘localguest’ as per Microsoft recommendation and by the Centre For Internet Security’s scoring tool.
 - Audit: Access of global system objects: Disabled
 - Audit: Use of Backup and Restore privileges: Enabled
 - Devices: Allow undock without have to log on: Disable
 - Domain member: Require strong (Windows 2000 or later) session key: Enabled. This is not a concern for computers operating in an exclusively Windows-2000-or-newer environment.
 - Interactive login: Do not display last user name in logon screen: Enabled.
 - Interactive login: Message text for users attempting to log on: This should contain a legal disclaimer as set by the client. An example of such a message would be:
 - This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement personnel.
 - Interactive login: Message title for users attempting to log on: This should contain a relevant title to accompany the disclaimer. A serviceable example would be ‘Warning’.
 - Interactive login: Number of previous logons to cache (in case domain controller is not available): 0.
 - Interactive login: Smart card removal behavior: This setting should be set to “Lock Workstation”.
 - Microsoft network client: Digitally sign client communications (always): Enabled.
 - [XP/2003] Microsoft network client: Digitally sign client communications (if server agrees): Enabled.
 - [2000] Microsoft network client: Digitally sign client communications (when possible): Enabled.
 - Microsoft network server: Digitally sign communications (always): Enabled.

- [XP/2003] Microsoft network server: Digitally sign communications (if client agrees): Enabled.
- [2000] Microsoft network server: Digitally sign communications (when possible): Enabled.
- Network access: Allow anonymous SID/Name translation: Disabled, as recommended by Microsoft and by the Centre For Internet Security's scoring tool.
- Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled, as per Microsoft's security analysis tool and recommendations
- Network access: Do not allow storage of credentials or .NET passports for network authentication: Enabled, to prevent credentials from being stored.
- [XP] Network access: Sharing and security model for local accounts: Set to "Classic".
- Network access: Shares that can be accessed anonymously: This list should be empty.
- Network security: Do not store LAN manager password hash value on next password change: Enabled, to prevent LM hashes from being stored.
- Network security: Force logoff when logon hours expire: Enabled.
- Network security: LAN Manager authentication level: This should be set to send NTLMv2 responses only.
- Network security: Minimum session security for NTLM SSP based (including secure RPC) clients: This should be set to 'Require NTLMv2'
- Network security: Minimum session security for NTLM SSP based (including secure RPC) servers: this should be set to 'Require NTLMv2'
- System Objects: Default owner for objects created by the Administrators group: This setting should be set to the Administrators Group.

Additional, non-default security policies must be installed for Windows XP and 2003 Server. For information on how to install these policies, see section 3.2, *Additional security components*.

TCP/IP related entries.

If any of the items listed below are missing, manually create them under the registry HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters.

All of these registry entries are DWORD values. Note that the name of the entry must be enclosed within brackets. After creating the missing entries restart the Local Security Policy editor.

- MSS: (DisableIPSourceRouting) IP Source Routing Protection Level: This option should be configured to always drop all source routed packets.
- MSS: (EnableDeadGWDetect) Allow Automatic Detection Of Dead Network Gateway: Disabled.
- MSS: (EnableICMPRedirect) Allow ICMP Redirects to Override OSPF Generated Routes: Disabled.
- MSS: (KeepAliveTime) How Often Keep-Alive Packets Are Sent (in milliseconds) : 300000 (5 minutes)
- MSS: (PreformRouterDiscovery) Allow IRDP to Detect and Configure Default Gateway Addresses: Disabled.
- MSS: (TcpMaxDataRetransmissions) How Many Times Unacknowledged Data is Retransmitted: 3 times

Miscellaneous Entries

If any of the items listed below are missing, manually create. Create the entry in the directory listed after the name of the item. All of the registry entries are DWORD values. Note that the name of the entry must be enclosed within brackets. After creating the missing entries restart the Local Security Policy editor.

- MSS: (NoDriveTypeAutoRun) Disable autorun for all drives: Enabled.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\
- MSS: (NoNameReleaseOnDemand) Allow the Computer to Ignore NetBIOS Name Release Requests Except from WINS Servers: Enabled.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\
- MSS: (SafeDllSearchMode) Enable Safe DLL Search Mode: Enabled.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\
- MSS: (ScreenSaveGracePeriod) The Time In Seconds Before The Screensaver Grace Period Expires: 0 seconds.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\

- Registry settings

Using the Registry Editor “regedt32” the following entries should be added or updated:

- HKLM\Software\Microsoft\DrWatson\CreateCrashDump: 0 to suppress crash dumps
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutorun: 255 to disable autorun on all drives
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutorun: 255 to disable autorun on all drives
- HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutorun: 255 to disable autorun on all drives
- HKLM\System\CurrentControlSet\Services\CDrom\Autorun: 0 to disable autorun on CD rom drives
- HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks: is set to an empty list, providing no shares
- HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect: 0 in order to disable the detection of dead gateways
- HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting: 1 in order to disable this behavior
- HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect: 0 in order to disable this behavior
- HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime: 300000 in order to match Microsoft’s security recommendations.
- HKLM\System\CurrentControlSet\Services\NetBt\Parameters\NoNameReleaseOnDemand: 1 to enable this behavior.
- HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery: 0 in order to match Microsoft’s security recommendations that this be disabled.
- HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect: 1 in order to match Microsoft’s security recommendations that this be enabled.

- HKLM\System\CurrentControlSet\Services\IPSec\NoDefaultExempt:1 to enable IPSec communications for Kerberos tickets
- HKLM\System\CurrentControlSet\Services\Lanmanserver\Parameters\Hidden: 1 to hide this machine from the computer browser
- HKLM\System\CurrentControlSet\Control\SessionManager\SafeDllSearchMode: 1 to force searching system folders first for dlls
- HKLM\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog: 1 (enable)
- HKLM\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog: 20, to allow 20 free connections for a given listening endpoint before a new thread is created.
- HKLM\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog: 320000 – this is the number of ‘quasi-free’ connections to allow.
- HKLM\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta: 10 – the number of additional connection to create at a time when more connections are needed.

8. File Permissions

Unless otherwise indicated, full permissions should be given to the users indicated below. A notable exception is the user 'INTERACTIVE' whose permissions should always be kept at the default level. Permissions on files listed below must be granted to only the users listed and to no others. Skip any files that do not exist.

- Windows\System32\at.exe - Administrators, SYSTEM
- Windows\System32\attrib.exe - Administrators, SYSTEM
- Windows\System32\cacls.exe - Administrators, SYSTEM
- Windows\System32\debug.exe - Administrators, SYSTEM
- Windows\System32\drwatson.exe - Administrators, SYSTEM
- Windows\System32\drwtsn32.exe - Administrators, SYSTEM
- Windows\System32\edlin.exe - Administrators, SYSTEM, INTERACTIVE
- Windows\System32\eventcreate.exe - Administrators, SYSTEM
- Windows\System32\eventtriggers.exe - Administrators, SYSTEM
- Windows\System32\ftp.exe - Administrators, SYSTEM, INTERACTIVE
- Windows\System32\net1.exe - Administrators, SYSTEM, INTERACTIVE
- Windows\System32\net.exe - Administrators, SYSTEM, INTERACTIVE
- Windows\System32\netsh.exe - Administrators, SYSTEM
- Windows\System32\rpc.exe - Administrators, SYSTEM
- Windows\System32\reg.exe - Administrators, SYSTEM
- Windows\regedit.exe - Administrators, SYSTEM
- Windows\System32\regedt32.exe - Administrators, SYSTEM
- Windows\System32\regsvr.exe - Administrators, SYSTEM
- Windows\System32\regsvr32.exe - Administrators, SYSTEM
- Windows\System32\rexec.exe - Administrators, SYSTEM
- Windows\System32\rsh.exe - Administrators, SYSTEM
- Windows\System32\runas.exe - Administrators, SYSTEM
- Windows\System32\sc.exe - Administrators, SYSTEM
- Windows\System32\subst.exe - Administrators, SYSTEM
- Windows\System32\telnet.exe - Administrators, SYSTEM, INTERACTIVE
- Windows\System32\tftp.exe - Administrators, SYSTEM, INTERACTIVE
- Windows\System32\tlntsvr.exe - Administrators, SYSTEM

For GEMS 1.18 and earlier, and GEMS 2.1: provide the "GEMS User" full access to the directory where GEMS is installed. This is usually "C:\Program Files\Global Election Systems\GEMS".

9. Registry Permissions

Using the Registry Editor “regedt32” the following keys permissions should be modified.

To modify the permissions right click on the registry entry and select “Permissions” from the menu. Then select the Advanced option and uncheck the “Inherit from parent...” option and then select “Copy” from the warning dialog that is displayed. Next remove any items not listed (do not set to deny) and then edit the permissions as listed. Any permissions other than Full or Read will need to be set using the advanced option in the permissions editor.

- HKLM\Software

Administrators	Allow Full
Creator Owner	Allow Full
System	Allow Full
Users	Allow Read

- HKLM\Software\Microsoft\Windows\CurrentVersion\Installer

Administrators	Allow Full
System	Allow Full
Users	Allow Read

- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies

Administrators	Allow Full
System	Allow Full
Authenticated Users	Allow Read

- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Ratings

Administrators	Allow Full
Users	Allow Read

- HKLM\Software\Microsoft\MSDTC

Administrators	Allow Full
System	Allow Full
Network Service	Allow Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Read
Users	Allow Read

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\SeCEdit

Administrators	Allow Full
System	Allow Full
Users	Allow Read

- HKLM\System

Administrators	Allow Full
Create Owner	Allow Full, Subkeys only
System	Allow Full
Users	Allow Read

- HKLM\System\CurrentControlSet\Enum

Administrators	Allow Full
System	Allow Full
Authenticated Users	Allow Read

For GEMS 1.18 and earlier, and GEMS 2.1:

- HKLM \SOFTWARE\Global Election Systems\GEMS
 - Administrators Allow Full
 - Create Owner Allow Full, Subkeys only
 - System Allow Full
 - Users Allow Read

For Response to California Conditions of Re-approval

Plan for Formatting and Clearing Program Storage on Voting System



**Revision 1.0
September 4, 2007**

Copyright

Plan for Formatting and Clearing Program Storage on Voting System
Copyright © 2007 Premier Election Solutions, Inc.
All Rights Reserved.

Important Notice

This document is the copyrighted property of Premier Election Solutions. Any reproduction, distribution, display, translation, or modification of any portion of this document without the express written authorization of Premier Election Solutions is prohibited. Additional copies may be purchased from Premier Election Solutions for a fee.

Premier Election Solutions, Inc.
PO Box 1019
Allen, TX 75013

Disclaimer

WARNING: The processes described in this document are mandated by the Secretary of State of California. Following these processes result in the permanent removal of voting records stored on the equipment and on the various computers involved. It is the responsibility of the Secretary of State of California and the jurisdictions and others following the described procedures to assure compliance with both Federal Law as well as the laws and regulations of the State of California regarding elections and record retention. Premier Election Solutions, Inc. strongly recommends that personnel, having appropriate training and skill, be used in performing the tasks below and that all computers and systems be fully archived using such back-up procedures as the Secretary of State may recommend. Such personnel should also meet any requirements for background investigations or other qualifications imposed by the Secretary of State of California. It is the responsibility of the Secretary of State and the jurisdictions and others following these processes to meet any California or Federal requirements, as appropriate, regarding physical security, logistical security and access control to election equipment so as to insure that the activities meet election security needs as well as computer security. Premier Election Solutions, Inc. does not express any opinion on the adequacy of any other such processes, regulations or other requirements established by the Secretary of State other than the fact that the security of computer or voting device is only one aspect of election security.

NO WARRANTIES OF ANY NATURE ARE EXTENDED BY THIS DOCUMENT. Any product and related material disclosed herein are only furnished pursuant and subject to the terms and conditions of a duly executed license or agreement to purchase or lease equipment. The only warranties made by Premier Election Solutions, Inc., if any, with respect to the products described are set forth in such license or agreement. Premier Election Solutions, Inc., does not accept any financial or other responsibility that may result from your use of the information in this document or software material, including direct, indirect, special, or consequential damages. You should be very careful to ensure that the use of this information and/or software material complies with the laws, rules, and regulations of the jurisdictions with respect to which it is used. Premier Election Solutions' products and product upgrades are subject to local statutory and certification requirements and are distributed according to customer contract provisions, need, and availability.

Trademarks

ASSURE™, AccuVote®, AccuView Printer®, BallotStation®, Central Tally System™, ExpressPoll®, GEMS®, Key Card Tool™, Optical Scan Accumulator Adapter™, UAID™, and VCProgrammer™ are trademarks owned by or licensed to Premier Election Solutions. All other trademarks are the exclusive property of their respective owners.
Part number: Not Applicable

Document History

Document Number	Revision	Date	Remarks
Not Applicable	1.0	September 4, 2007	Initial Release

Table of Contents

1	Introduction	1
1.1	Purpose	1
1.2	Audience.....	1
1.3	Document Guidelines	1
1.4	Referenced Document List.....	1
2	Product List.....	2
2.1	Products with Program Storage	2
2.1.1	Authenticity and Integrity Model (AIM).....	2
2.1.2	Election Management Hardware (Air Gap Model).....	2
2.1.3	Accuvote-TS	2
2.1.4	Flash Disk Memory Cards (PCMCIA).....	2
2.1.5	AVOS Optical Scan Memory Cards.....	2
3	Overview	3
3.1	Authenticity and Integrity Model (AIM)	3
3.1.1	Gems Server.....	3
3.1.1.1	Trusted Build Digital Signatures	3
3.1.1.2	Election Definition Digital Signatures	4
3.1.1.3	Election Results Digital Signatures	4
3.1.2	Work Station / Laptop (AIM)	4
3.2	Election Management Hardware (Air Gap Model)	5
3.2.1	GEMS Server 1.....	5
3.2.2	GEMS Server 2.....	5
3.2.3	Work Station / Laptop	5
3.3	Accuvote-TS (TSX).....	5
3.4	PCMCIA Memory Cards.....	6
3.5	AVOS Optical Scan Memory Cards	6
4	Implementation	7
4.1	Authenticity and Integrity Model (AIM)	7
4.2	Election Management Hardware (Air Gap Model)	7
4.2.1	Re-Installation GEMS Server 1 and 2	7
4.2.2	Re-Installation Work Station / Laptop	7
4.3	Re-Installation TSX.....	8
4.4	Clearing PCMCIA Memory Cards	8
4.5	Clearing AVOS Optical Scan Memory Cards	8
4.5.1	Clearing AVOS Memory Card Procedure Option 1	8
4.5.2	Clearing AVOS Memory Card Procedure Option 2	8
5	Discussion.....	9

1 Introduction

1.1 Purpose

This document is intended as a plan that outlines the applicable procedure to clear all program storage from the Premier Election Solutions voting system as required by the California Secretary of State per the Conditions of Re-approval.

1.2 Audience

This document has been prepared for the California Secretary of State and State Elections Division Staff.

1.3 Document Guidelines

- The California Secretary of State's office ("State") has indicated that only certain voting system functionalities, which are resident on computers or devices, are subject to having their Program Storage cleared or re-formatted when implementing the Air Gap Model. The voting system functions are listed below.
 - Creation of election definitions
 - Capturing of voting results
 - Electronic transmission voting results
 - Archival or storage election definitions or voting results
 - Clearing of Voting System Program Storage from (PCMCIA) flash disk memory cards

- The State has indicated that an alternative security model, other than the Air Gap Model, could be considered. Therefore, an "Authenticity and Integrity Model" (AIM) is also proposed in this document. The AIM proposal as outlined in this document appears to be as viable as the Air Gap Model, and AIM also appears to be more economical for jurisdictions to implement. The last section of this document contains a discussion on the viability and economics of the two models.

1.4 Referenced Document List

- GEMS Server Configuration Guide Revision 11.0.pdf
- GEMS 1.18 Server Administration Guide Revision 3.0.pdf
- AccuVote-OS Precinct Count 1.96 User's Guide Revision 8.0.pdf

2 Product List

2.1 Products with Program Storage

2.1.1 Authenticity and Integrity Model (AIM)

- GEMS Server
- Work Station / Laptop

2.1.2 Election Management Hardware (Air Gap Model)

- GEMS Server 1
- GEMS Server 2
- Workstation-Laptop

2.1.3 Accuvote-TS

- Model TSX

2.1.4 Flash Disk Memory Cards (PCMCIA)

- Model – All

2.1.5 AVOS Optical Scan Memory Cards

- Model - All

3 Overview

3.1 Authenticity and Integrity Model (AIM)

The Authenticity and Integrity Model for election management uses digital signature technology to create manifests of the operating system and application file hashes that are resident on a trusted build of a Voting System server, work station, or laptop computer. Election activity including creation of election definitions, election results capture, and reporting can securely be performed using the model on just one (1) computer platform. Clearing of Voting System Program Storage from removable media can be performed on work stations or laptops.

3.1.1 Gems Server

Once a trusted build is initially performed on the GEMS Server, an image is taken of the hard drive so that in the event of integrity checks failing, the GEMS server can be rebuilt using that trusted image.

There are three (3) categories of static files to which digital signatures can be applied. Those categories are Trusted Builds, Election Definitions, and Election Results. The integrity check can be conducted at any time.

The digital signatures can be computed and compared to trusted values by third party software that is commonly used for computer forensics. One such package is called MaresWare, which was developed by Dan Mares. The Georgia Center for Elections Systems at Kennesaw State University (“KSU”) uses this software package with their manifest of files to verify the integrity of the GEMS servers installed in each jurisdiction in their state. KSU also verifies static operating system files and also checks for the presence of any extraneous files that should not be on the GEMS server.

The program can be operated with a GO/NO-GO criteria established by the State. A local election official can operate the program by simply executing it from a CD-ROM. The program reports whether the criteria was a GO or a NO-GO. If the integrity check fails, then the software produces a report to a floppy disk that specifies the reason for the failure. That report can then be examined by the State to determine the reasons for the discrepancies.

3.1.1.1 Trusted Build Digital Signatures

The file hashes or digital signatures of the trusted build / installation of the GEMS server are the file types that are installed by, or used by the voting system, and those files which are static in nature. This includes files such as, executable (.exe), dynamically linked libraries (.dll), application resource files, and operating system files.

- Voting System Integrity is ensured by regenerating the file Digital Signature manifest before and during the election process and comparing all of the generated Digital Signature manifests with the trusted builds Digital Signature manifest.
- The trusted builds manifest is kept for public record.

3.1.1.2 Election Definition Digital Signatures

Files which are generated during the creation of election definitions, database backup files (.gbf), on the GEMS server should also be hashed at the end of each session.

- Generating Digital Signatures of backup files ensures subsequent authenticity and integrity of the election definition.
- Prior to starting a new session, verification of the intermediate election definition backup file should be performed by comparing a new Digital Signature manifest with the prior Digital Signature manifest.
- The file hashes taken during this process are to be kept for public record.

3.1.1.3 Election Results Digital Signatures

At the end and periodically during the voting system's capture of election results from voting terminals and or from the absentee ballot scanning process, database backup files (.gbf), on the GEMS server should be generated and should be hashed producing Digital Signature manifests to provide election results integrity and authenticity.

- Generating Digital Signatures of backup files that have intermediate and final election results should be performed to guarantee election integrity.
- The file hashes taken during this process are kept for public record.

3.1.2 Work Station / Laptop (AIM)

A single or possibly more, Workstations or Laptops are used to delete previous elections from removable media, (PCMCIA memory cards only).

* **Note: The Authenticity and Integrity Model could be applied to any number of Voting System Computers used to clear Program Storage from PCMCIA Removable Media.**

- These computers should be equipped with external PCMCIA card reader / writers. As PCMCIA connectors in laptops are only meant to facilitate approx. 10,000 insertions, it is recommended that external PCMCIA reader/writers be used so that they can be replaced when worn without requiring the replacement of the computer.
- These computers should only be loaded with the basic operating system.
- No third party software should be loaded except that required to operate the PCMCIA card reader / writer.
- These computers should be dedicated to performing this function and not used for alternate purposes.

3.2 Election Management Hardware (Air Gap Model)

The Air Gap model for election management requires a minimum of three (3) physically separate computers each performing independent operations related to the election process.

3.2.1 GEMS Server 1

The first server is used to create the election definition, ballot templates and to download data to the vote capture memory cards. This computer would be a trusted build of the GEMS Server. Once a trusted build is initially performed on the GEMS Server, an image is taken of the hard drive so that in the event of the integrity of the GEMS server is questioned; the GEMS server can be rebuilt using that trusted image.

Major actions performed on the same server subsequent to creation of the election database:

- Postscript or Portable Document Format (pdf) files are generated and used to produce ballots for paper based optical scan devices.
- Downloading of vote center specific database portions from the jurisdiction wide database to removable media. The vote center database portion can be downloaded to either:
 - PCMCIA flash memory cards, for use in a TSX voting terminals.
 - Optical scan memory cards, for use in AVOS voting terminals.

3.2.2 GEMS Server 2

The second server is used for the uploading of election results from TSX, AVOS, and EMP devices and producing election results reports. GEMS Server 2 can also be used as a Central Count server. Central Count optical scanning devices can be attached and used to scan ballots, typically absentee ballots, sending ballot images to GEMS Server 2 for tabulation. The hard drive image from the first GEMS server can be used to initially configure the second GEMS Server.

Note: AccuVote Central Count scanners do not tabulate election results. They simply scan a ballot image and pass it onto the Central Count server for tabulation.

Major actions performed on GEMS Server 2 subsequent to election results uploading and Central Count tabulation:

- Election result reporting (GEMS Summary report)
- Election Canvass and reporting (GEMS Statement of Votes Cast report)

3.2.3 Work Station / Laptop

The third, and possibly more, Workstations or Laptops are used to delete previous elections from removable media, (PCMCIA memory cards only).

- Because PCMCIA connectors in laptops are only meant to facilitate approx. 10,000 insertions, it is recommended that external PCMCIA reader/writers be used so that they can be replaced when worn without requiring the replacement of the computer.
- These computers should only be loaded with the basic operating system.
- No third party software should be loaded except that required to operate the PCMCIA card reader / writer.
- These computers should be dedicated to performing this function and not used for alternate purposes.

3.3 Accuvote-TS (TSX)

The TSX DRE voting terminal uses internal flash memory as secondary program memory storage.

3.4 PCMCIA Memory Cards

The TSX DRE voting terminal uses PCMCIA cards as primary program memory storage.

3.5 AVOS Optical Scan Memory Cards

The AVOS precinct ballot counter uses optical scan memory cards as primary program memory storage.

4 Implementation

4.1 Authenticity and Integrity Model (AIM)

The Authenticity and Integrity Model should be employed by the election official and the process should have oversight from the State. One possible implementation is cited below.

- The third party “Manifest” application, chosen by the State, suitable for the generation of the voting systems Digital Signature manifests, would be housed on a CD and kept in a secure location, one which could not be accessed by any single person, in each jurisdiction.
- A user account should be created that is used only for the purpose of performing the generation of these digital signatures.
- Before the Manifest application would be allowed to run on the GEMS Server, the user must log into the GEMS server. The AIM user account is a user account with one additional privilege.
 - Ability to execute the Manifest application
- At any time a Digital Signature manifest is created by the Manifest application a log entry of the activity would be generated in the Windows System event log and also in a separate Manifest log.
- Any time the AIM user logs into the GEMS Server a log entry of the activity would be generated in the Windows System event log and also in a separate Manifest log.
- Two or more copies of the Manifest data file along with the Manifest log file are written to separate CD’s.
- Both the Manifest application CD and one Manifest data CD are re-secured.
- The remaining archival CD’s are maintained by a chain of custody which the state determines.

4.2 Election Management Hardware (Air Gap Model)

All GEMS servers may be reinstalled to clear program storage. Only qualified IT personnel should attempt to perform a GEMS server re-installation. The election administrator should oversee the process to ensure that all appropriate databases are preserved.

- * **BACKUP ALL ELECTION DATABASES TO CD**
- * **PERFORM THE *COMPLETE* BACKUP AT LEAST TWICE**

4.2.1 Re-Installation GEMS Server 1 and 2

- Format all hard drives. Typically a raid 5 configuration.
- Install operating system – Currently:
 - Windows Server 2000 or Windows Server 2003
- Harden server security.
 - Reference: GEMS Server Configuration Guide Revision 11.0.pdf
- Install GEMS, third party software, and peripherals.
 - Reference: GEMS 1.18 Server Administration Guide Revision 3.0.pdf

4.2.2 Re-Installation Work Station / Laptop

All work stations and laptops used to delete previous elections form removable PCMCIA media may be reinstalled to clear program storage. Only qualified IT personnel should attempt to perform the work station / laptop re-installation. The election administrator should oversee the process.

- Format all hard drives. Typically a single hard drive.
- Install operating system – Typically:
 - Windows XP Professional or Windows 2000 Workstation

- Harden computer security.
 - Reference: GEMS Server Configuration Guide Revision 11.0.pdf

- Install third party software for the PCMCIA card reader / writer if needed.
 - Reference: vendor's documentation for the card reader / writer.

4.3 Re-Installation TSX

The TSX DRE voting terminal may be reinstalled to overwrite program storage contents from previous installations. Only qualified election personnel should attempt to perform a TSX DRE re-installation. The election administrator should oversee the process.

- Install the TSX boot loader and Windows CE operating System.
 - Reference: TBD
- Install the TSX Ballot Station application.
 - Reference: AccuVote-TSx Hardware Guide Revision 8.0.pdf
 - Appendix D: System Acquisition and Installation

4.4 Clearing PCMCIA Memory Cards

Use the Election Management Systems laptop / workstation, described in the Air Gap Model above, to reformat the PCMCIA cards.

- PCMCIA cards are reformatted using the installed operating systems 'Format' utility.
- PCMCIA cards should be formatted using the FAT32 file system.
- IDs placed on the PCMCIA cards at formatting must be unique to that card.

4.5 Clearing AVOS Optical Scan Memory Cards

Use an AVOS unit to clear optical scan memory cards.

4.5.1 Clearing AVOS Memory Card Procedure Option 1

To clear the AVOS optical scan memory card first reset the card to Pre-Election Mode:

- Reference: AccuVote-OS Precinct Count 1.96 User's Guide Revision 8.0.pdf
 - Section 14.9. Resetting the memory card to Pre-Election Mode

From Pre-Election Mode clear the memory card:

- Reference: AccuVote-OS Precinct Count 1.96 User's Guide Revision 8.0.pdf
 - Section 14.10. Clearing the memory card

4.5.2 Clearing AVOS Memory Card Procedure Option 2

Alternately, the optical scan memory cards can be cleared by conducting a Memory Card Test in the System Diagnostic Mode.

- A data pattern will overwrite all data on the card including the format.
- When downloading election data to the card at a later date, the system will automatically detect the absence of a format and will automatically format the memory card before the data download begins.

5 Discussion

Imaging of a GEMS Server hard drive after the initial trusted build is configured on the computer is an efficient method of providing for re-installation after each election. Re-installing the operating system, hardening the configuration, and re-installing each application software package can be a tedious process that provides opportunities for errors to be made along the way. With a hard disk image of a trusted build, in which the State provided oversight, the State can be confident that the configuration will be capable of re-installation without any alterations being made to that trusted build. A digital signature can be generated on the image itself to verify its integrity before it is used for each re-installation. Third party software, such as, Norton Ghost can be used to facilitate these re-installations.

Either model methodology described above can be used to ensure the integrity and authenticity of a GEMS Server. However, the Air Gap model uses two (2) GEMS servers and the AIM process uses only (1) GEMS Server. To supply a back up system, jurisdictions would need four (4) GEMS Servers in total to accommodate the Air Gap Model. Currently, jurisdictions have only one (1) GEMS Server with a possible secondary GEMS server for backup. Implementing the Air Gap Model would mean requiring jurisdictions to purchase new computers which would likely be different platforms from the ones they originally purchased. To use hard drive imaging as an effective method of re-installation, the computer platforms need to be the same. To implement the Air Gap Model with backup servers would likely require jurisdictions to scrap their existing GEMS Servers and purchase four (4) new identical computer platforms.

In the Air Gap Model, it is assumed that the first GEMS server with its trusted build is never tampered with; however, to verify its integrity, there should be audits performed on the configuration and the files installed on that GEMS Server. To verify the integrity of that GEMS Server, it is likely that digital signatures would need to be generated from the files on the system and compared to digital signatures that were generated from the initial trusted build. Otherwise, how could the State be sure, over time, that the first server still matched its initial trusted build?

If the same manner of verification used in the AIM methodology would also need to be used to audit the first GEMS Server in the Air Gap Model, then it seems that the AIM methodology, using only one (1) server, is just as viable as the Air Gap Model using two (2) servers. In addition, the AIM methodology is a more economical path for jurisdictions with less opportunity for operator error.

Development Administration

Updating Security of Microsoft[®] Windows[®] on GEMS[®] Servers



Revision 1
August 30, 2007

Copyright

© 2007 Premier Election Solutions, Inc.,

All Rights Reserved

Important Notice

This document is the copyrighted property of Premier Election Solutions. Any reproduction, distribution, display, translation, or modification of any portion of this document without the express written authorization of Premier Election Solutions is prohibited. Additional copies may be purchased from Premier Election Solutions for a fee.

Premier Election Solutions, Inc.
PO Box 1019
Allen, TX 75013

Disclaimer

The information in this document is provided 'as is' and without warranty. Premier Election Solutions will not be liable for any incidental, consequential, or other damages of any type or nature, resulting from the provision or use of the information contained herein. All information is subject to change at any time without notice. Users of this document assume sole responsibility for their use of the information contained herein, as well as any products, software, or other materials that may be provided by Premier Election Solutions. Care should be exercised by such users to assure compliance with all applicable laws, rules, and regulations.

1. Introduction

This document describes the process that is used to obtain the latest security updates and patches for Microsoft Windows operating systems (2000, XP and 2003) for operation on GEMS Servers supplied and configured by Premier Election Solutions, Inc. Recommendations from Premier for Microsoft updates that are applicable to GEMS Servers are based on the assumption that the GEMS Server is never connected to the Internet.

Audience

This document is intended for Premier Election Solutions (Premier) staff responsible for building, verifying, shipping and supporting customer GEMS servers. It may also be used as a reference by qualified, customer IT personnel to construct their own GEMS servers or to update those servers in the field.

NOTE: The information contained in this document is for reference only. It is recommended that each jurisdiction consult with their State Election Authority in respect to applicable laws, regulations, procedures and other guidelines, which may impact how this information is used.

Installing the latest security updates for Windows 2000 server and Windows XP

On a monthly basis, Premier will review Microsoft's **TechNet Security Center** website at <http://www.microsoft.com/technet/security/default.msp> for the latest security updates issued for that particular month. Further, Premier will be automatically notified via email in the event new critical updates are released by Microsoft through the **Microsoft Technical Security Notification Services**.

Initial assessment by Premier will determine which updates are relevant and pertinent to the security and operation of the GEMS Server configuration. The relevant updates will be downloaded from Microsoft and tested for compatibility with the GEMS Server configuration. Once testing has proven successful, the identification of the relevant Microsoft updates will be distributed to Premier customers and state election authorities via Premier's Product Advisory Notice (PAN) process.

Distribution of the updates will be dependent on the procedures established by the State Election Authority for a jurisdiction. Premier can copy the relevant updates onto write-once media and distribute to jurisdictions if authorized by the jurisdiction's State Election Authority. Requests for the relevant updates on media can be placed through the Premier HelpDesk (866.307.7689).

State of California

USE PROCEDURES

Premier Election Solutions, Inc.

These procedures are proposed for adoption by the California Secretary of State pursuant to Elections Code sections 19200 and 19205 and shall regulate and govern the use of Premier Election Solutions AccuVote®-OS and AccuVote®-TSX (Touch Screen) at all elections governed by the California Elections Code.

These procedures shall be effective upon approval by the Secretary of State and shall be used in conjunction with all other statutory and regulatory requirements. Insofar as feasible, all procedures prescribed herein shall be carried out in full view of the public.

These procedures constitute a minimum standard of performance. They are not intended to preclude additional steps being taken by individual election officials to enhance security and reliability of the electoral process.

Submitted

September 17, 2007

Table of Contents

Table of Contents	i
1. Introduction	1
1.1. System description and components.....	1
1.2. Terms and Definitions.....	3
2. Ballot Definition	13
2.1. Overview.....	13
2.2. Paper and printing specifications.....	13
2.3. Layout requirements and specifications.....	13
3. System Installation and configuration	14
3.1. Hardware requirements and specifications.....	14
3.2. Hardware and network setup and configuration.....	14
3.3. Acceptance Testing.....	15
3.4. Software and firmware upgrades.....	17
4. Election Setup and Definition	18
4.1. Global Election Management System (GEMS).....	18
4.2. AccuVote-OS Testing.....	19
4.3. AccuVote-TSX Testing.....	23
4.4. AccuVote-OS and AccuVote-TSX Audit Log Retention.....	26
4.5. Public Logic and Accuracy Board and certification of testing.....	27
4.6. Ballot tally programs.....	27
4.7. Election Observer Panel.....	27
4.8. Hardware maintenance and preparation for use.....	27
5. Polling Place Procedures	29
5.1. Precinct supplies, delivery and inspection.....	29
5.2. Polling Place Setup.....	30
5.3. Opening the polls.....	31
5.4. Polling place procedures.....	32
5.5. Special needs voters.....	35
5.6. Provisional voters.....	36
5.7. Closing the polls and vote reporting.....	37
5.8. Securing audit logs and backup records.....	39
5.9. Troubleshooting and problem resolution.....	39
6. Absentee/Mail Ballot Procedures (central tabulation)	45
6.1. System startup and pre-tabulation report procedures.....	46
6.2. Tabulation procedures.....	46
6.3. Post tabulation report and shutdown procedures.....	47
7. Semi-Official Canvass Tabulation and Reporting	48
7.1. System start-up and pre-tabulation reports.....	48
7.2. Processing vote reports.....	50
8. Official Canvass and Post-Election Procedures	51
8.1. Election Observer Panel.....	51
8.2. Canvassing precinct returns.....	51
8.3. Canvassing Absentee returns.....	52
8.4. Canvassing provisional ballots.....	52
8.5. Canvassing write-in votes.....	53
8.6. Manual recount procedures.....	54
8.7. Handling ballot exceptions.....	54
8.8. Post election logic and accuracy testing.....	56
8.9. Final reporting of official canvass.....	56
8.10. Backup and Retention of election material.....	56

9.	Manual Recount procedures	58
10.	Security	60
10.1	Physical security of system and components	60
10.2	Logical security of system and components	68
10.3	Security procedures for central processing	70
10.4	Security procedures for polling place	71
10.5	Audit trails	71

1. Introduction

1.1. System description and components

This manual of USE procedures is for jurisdictions using the Premier Election Solutions, Inc. (Premier) as certified by the State of California. It is to be used in conjunction with the user guides distributed at the time of upgrade. Additional copies, if needed, may be obtained from Premier. The system components are listed below:

- GEMS® Software Version 1.18.24
- AccuVote®-TSX Ballot Station Version 4.6.4
- Key Card Tool Version 4.6.1
- Voter Card Encoder Version 1.3.2
- VC Programmer 4.6.1
- AccuVote®-OS firmware version 1.96.6
- AccuVote®-OS Central Count firmware version 2.0.12
- AccuFeed

An overview of each component follows:

The Global Election Management System (GEMS)® 1.18.24 Election Management System is a Microsoft Windows-based election management and tabulation software that allows complete control of the election process, from precinct/district set-up, to race definition, tabulation and reporting. With GEMS software you can combine the programming of absentee or mail ballots and create the ballot layout of the optical scan and touch screen units all in one programming process. GEMS 1.18.24 software completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N-1-06-22-22-001.

The Ballot Station Software firmware 4.6.4 is designed to run exclusively on the Premier AccuVote®-TSX touch screen voting device with the AccuView Printer® Module (AVPM). This software allows a voter to interact with the voting device by touching the unit's touch screen panel for the capture of their vote. The Ballot Station software 4.6.4 incorporates changes from previous releases to utilize the AVPM.

The Key Card Tool 4.6.1 is a PC based software application designed to enhance the security provided by the AccuVote-TSX units used in an election. The Key Card Tool application, when used in conjunction with an external smart card reader device, allows the user to create a smart card encoded with user-defined security codes or keys. The Key Card may be used to encode the security key values on the election's smart card reading equipment. These values can be changed per election. The Key Card Tool 4.6.1 version completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N-1-06-22-22-001.

The Voter Card Encoder 1.3.2 is a device designed to encode voter access cards for the purpose of activating ballots on the AccuVote-TSX units used in an election. The Voter Card Encoder is encoded with "Master" voter access cards created from the AccuVote-TSX Ballot Station database application. The Voter Card Encoder can be pre-programmed with up to eight different ballot styles. Poll workers can encode voter access cards for each voter with the appropriate ballot style in their voting location. The Voter Card Encoder 1.3.2 completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N-1-06-22-22-001.

The VCPProgrammer 4.6.1 is a PC based application that, when used with an external smart card reading device, can be used to create voter access cards for use on AccuVote-TSX Ballot Station units configured for an election.

A file exported from the GEMS election database supplies the information required by the application to create voter access cards. When this file has been made available to VCPProgrammer, the application can be used to identify the precinct and party associated with the ballot to be copied onto a voter access card for a voter.

VCPProgrammer may be configured to interface with a voter registration system during a live election. When configured this way, the application automatically identifies the precinct and party associated with the ballot to be copied onto a voter access card when voter information is updated in a file generated by the registration system and referenced by VCPProgrammer. The VCPProgrammer 4.6.1 completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N-1-06-22-22-001.

The AccuVote®-OS Optical Scan (model D) with 1.96.6 firmware is a mark sense paper-based voting device. It offers a precinct count and absentee voting solution that can be configured as a stand-alone system in a polling environment. Each precinct count AccuVote-OS unit is loaded with a memory card programmed with ballot information for the corresponding polling location or precinct(s). The results of ballots scanned by the AccuVote-OS are tallied to the memory card, and these results are uploaded to the host computer at the close of election. The AccuVote-OS will accommodate three different size ballots, all 8 ½ X 11", 14", and 18" ballots in length. Ballots can be fed into each unit in any direction or orientation. Both sides of the ballots will be read and recorded at the same time. The AccuVote-OS also has the option of being programmed to reject any over-voted, fully blank ballot or under-voted races if required by the State. The AccuVote-OS (model D) with firmware version 1.96.6 completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N-1-06-22-22-001.

AccuVote®-OS Central Count firmware 2.0.12 is a compact and, scaleable batch ballot processing solution employing the AccuVote-OS ballot counting device configured with a Central Count firmware, linked over a local area network connection to the GEMS election management server. Ballots scanned by the AccuVote-OS Central Count unit pass card ID information to the GEMS server over the local network. The GEMS server confirms the ballot identification, and returns a ballot mask to the AccuVote-OS Central Count device. Using the ballot mask, valid voting positions are uploaded for the ballot to GEMS.

The AccuVote-OS Central Count is used for processing large volumes of mail ballots, such as absentee ballots. Since the ballot information as well as the tally files is stored on the GEMS server, central count does not limit the number of unique ballot styles processed in a single processing session. AccuVote-OS Central Count mode allows any ballot type to be fed into the AccuVote-OS without any presorting of ballots. All that is required is that the vote center in which ballots are counted is logically associated with all the election precincts to the vote center in the GEMS software database.

AccuVote-OS Central Count may be configured with multiple AccuVote-OS Central Count units linked to the GEMS server in either a local area network configuration or using Windows Remote Access Server (RAS).

The AccuVote-OS Optical Scan Central Count 2.0.12 completed ITA testing under the 2002 Voting System Standards, and is included under the assigned NASED System Number of N-1-06-22-22-001.

The AccuFeed Ballot Feeder is a mechanical ballot feeding device which can be used with the AccuVote-OS. This hardware allows the operator to place stacks of ballots into the input

stacker tray which are fed into the AccuVote-OS optical scan unit. The AccuFeed ballot feeder does not tabulate or scan the ballot. The unit functions to feed the next ballot to the AccuVote-OS unit. The AccuFeed ballot feeder is placed on top of the AccuVote-OS in the Central Count configuration and the ballot feed function is controlled by the AccuVote-OS via a single optical coupler.

1.2 Terms and Definitions

This section contains a comprehensive glossary of terms used with the AccuVote-OS, the AccuVote-TSX, and related functions in GEMS, in alphabetical order.

“Absentee Voter”

A voter who votes at a location other than their polling place by means of paper ballot, or by means of an electronic ballot at the election office or a designated satellite location.

“AccuVote Server”

The console window used in GEMS for programming AccuVote-OS and AccuVote-TSX election media and uploading election results.

“AccuVote-OS”

The AccuVote-OS (AVOS) unit consists of optical scanner hardware and software that accepts and tallies votes, prints reports, and rejects votes based on specified conditions (e.g., overvotes, blank voted ballots)

“AccuVote-TSX”

The AccuVote-TSX (AVTSX) unit consists of hardware and software for the electronic ballot station functions, which includes the selection of the ballot, the detecting and recording voter choices, and the printing of reports. Additionally, the AVTSX prints out a voter verifiable paper trail on the AccuVote Printer Module (AVPM) for a voter to review the voted selections prior to casting a ballot on the AVTSX.

“Accessible Voter Verifiable Printed Audit Trail (AVVPAT)”

The Accessible Voter Verifiable Paper Audit Trail refers to the AccuView Printer Module’s (AVPM) printed summation of a voter’s choices that the voter verifies against the electronic ballot.

“Administrator Card”

A special smart card programmed to allow complete access to all functions on the AccuVote-TSX ballot station. It is NOT intended for poll worker use and is NOT needed for closing the polls and for initiating the printing of election results.

“Administration Screen”

The various functions of the administrative window on the AccuVote-TSX designed only to be accessed at specified points in the election process. Functions on this screen include: Start Election, End Election, Transfer Polling Data, Exit Administrative State, and Shutdown System.

“Archive”

Election and election results files preserved for back-up or election recovery purposes.

“Archiving of Election Data”

Once the transport media results have been entered on the host, the removable disk is archived. Verification of tabulations can be re-created by comparing records from the fixed storage on the AccuVote-TSX with the results from the transport storage on the disks.

“Audio Ballot”

The ballot composed in audio format, containing identical race and candidate content and ordering as the corresponding visual ballot, and including operational instructions for the selection of candidates and ballot measures, traversing the race list, definition of write-in candidates, and printing and casting of ballots.

“Audit Log”

An audit record of the audit transactions on the AccuVote-OS and the AccuVote-TSX. The audit log provides the supporting documentation for verifying the correctness of the reported results. The audit function presents a record of all system activity.

“AccuView Printer Module (AVPM)”

The AccuView Printer Module (AVPM) that attaches to the AccuVote-TSX unit for printing the Accessible Voter Verifiable Paper Audit Trail (AVVPAT).

“Backup Flash Memory”

The internal “flash” memory storage location on the AccuVote-TSX, where elections and election results are stored.

“Ballot”

A ballot refers to a rotated ballot style.

“Ballot ID”

A unique identifier number assigned to the ballot.

“Ballot Serial Number”

A unique serial number identifying a voted AccuVote-TSX ballot.

“Base Precinct”

Any largest area of a jurisdiction not intersected by district boundaries.

“Ballots Cast”

The total number of ballots cast on either an individual AccuVote-TSX or at a polling location, or on the GEMS host accumulation/reporting system.

“Ballot Station Software”

A single integrated software program residing on the AccuVote-TSX motherboard that displays, processes, reports, and transfers electronic ballot information.

“Blank Voted”

A ballot with no voter selections in any race, question, or issue.

“Button”

An object on the GEMS or the AccuVote-TSX user interface which is touched in order to activate a function.

“Candidate”

An individual running for office, for whom voters have the opportunity to vote on a ballot.

“Cast Ballot Button”

Button that is touched when the voter wishes to cast their ballot after all desired selections have been made and verified on the AVPM..

“Challenge Board”

The function used to review challenged / provisional ballots.

“Challenged or Provisional Ballot”

A ballot corresponding to a voter whose right to vote at a polling location has been challenged or a voter who insists that they be allowed to vote at the polling place in question. Challenged or provisional ballots are reviewed by jurisdiction administration prior to being released for counting or rejection.

“Copy”

The number of times a memory card or election media has been programmed without ballot layout having changed.

“Count”

A field display on the AccuVote-TSX to indicate either the number of ballots counted in the current election, or the total number of ballots counted since the manufacture of the AccuVote-TSX. The first is an Election Count and the second count is a System Count.

“Current Candidate”

The candidate currently selected on either the visual or audio ballot.

“Current Race”

The race containing the current candidate or ballot measure.

“Central Tabulating System”

Also referred to as GEMS. The computer system that reads the votes from the AccuVote-OS and AccuVote-TSX removable media, then tabulates the votes from all polling places (either satellite, central or precinct locations).

“Closed Primary”

An optional ballot criterion for conducting primary elections in which voters affiliated with a particular party may vote only for that party’s candidates.

“Contest”

The aggregate of candidates who run against each other for a particular office, or ballot measures.

“Dynamic Host Configuration Protocol (DHCP)”

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a DHCP server to automatically assign an IP address to an individual computer's TCP/IP software. DHCP assigns a number dynamically from a defined range of numbers (i.e., a scope) configured for DNS servers or WINS servers.

“Download”

The programming of election and ballot information onto the removable storage media for the AccuVote-OS and AccuVote-TSX.

“Election Counter”

The total number of ballots cast on an AccuVote-TSX during a specific election. Also known as the Public Counter.

“Election Name”

The name of the election programmed to election media.

“Electronic Ballot”

The electronic ballot is displayed with the appropriate candidates and issues presented on a touch screen for the voter to make choices and record his/her votes.

“Global Election Management System (GEMS)”

The backbone of the election system that provides the functionality for ballot definition and layout, the downloading and uploading of memory cards and the tabulation and reporting of votes. Also known as GEMS.

“Header”

Text information that appears on the ballot identifying the race title, question and issue description, as well as the number of selections available to the voter for the race.

“Hide Ballot”

The visually impaired ballot station option to hide the visual portion of the ballot as the audio ballot is played. This option is programmed to the voter smart card.

“High Contrast”

Ability to change the AccuVote-TSX presentation to black and white for low vision voters.

“Host Computer”

The GEMS computer, interfacing with GEMS clients and voting devices.

“Host Name”

The name or IP address of the GEMS host computer.

“Key Card”

The ‘Key Card’, created using the Key Card Tool that can be used to encode the security key values on the election's smart card reading equipment.

“Key Card Tool”

The Key Card Tool, a stand-alone application, that allows the user to create a smart card encoded with user-defined security codes or *keys*, and is also used to encode supervisor and administrator type smart cards with the election’s security key. The Key Card Tool is also used to update the card’s supervisor and administrator password.

“Keypad”

A telephone-style keypad used to enter commands in the audio ballot on the AccuVote-TSX.

“Language”

A ballot display selection available on the AccuVote-TSX, which allows the voter to select a ballot in the language of their choice, (e.g. English, Spanish, Chinese, Japanese, Vietnamese, Tagalog, Korean, and French). These are languages that have been used on the AccuVote-TSX. Languages are defined in the GEMS ballot layout software application.

“Large Text”

The ability to increase the size of ballot text for the benefit of visually impaired voters on the AccuVote-TSX.

“Last Oval or First Oval Deck”

A test deck used in an optical scan election. This consists of a single ballot card per precinct with either the first candidate or the last candidate in a race marked for each race. This deck or card is specific to a precinct and is run thru the corresponding precinct memory card. The purpose of this test is to check that the precinct IDs and ovals on the ballot match the expected data format of the precinct memory card for the precinct optical scanner or central count optical scanner. This test is used to populate a count into each precinct to ensure database version control has been maintained, that all precincts and memory cards match the GEMS database, and that data is accurately flowing between the precinct or central count scanners and the GEMS host system. This test and test deck are not sufficient as a total test and shall be used in conjunction with the Logic and Accuracy test decks (LA5, LAn, or LAmx).

“Logic and Accuracy Deck (5 or n or max)”

A test deck comprised of optical scan ballots that is used to test the logic of a precinct memory device in the AccuVote-OS or an absentee precinct using an AccuVote-OS device in central count mode. This deck can be ordered to give a 1,2,3,4,5 pattern to candidates in a race. For example, if there are seven candidates and a write-in – eight ovals in the race – an LA5 deck would give a 1,2,3,4,5,1,2,3 pattern. This deck can be ordered with any N number of the pattern. This deck can also be ordered as an “LA max” deck. In this case, the largest number of candidates on the ballot will define the “maximum” number of the pattern. If there are 15 candidates, then the deck would consist of 1 ballot for the 1st candidate, 2 ballots for the 2nd candidate, etc., up to the 15th candidate, which would have 15 ballots voted for the last candidate. This deck would have a total of 120 ballots. As the county determines that decks are getting too large, they may use an LA5 deck to simply assign a 1,2,3,4,5,1,2,3,4,5,1,2,3,4,5 pattern to large candidate races.

“Memory Card”

A solid state memory device utilizing industry standards for data storage of election and ballot information. It is a removable electronic media containing the election definition for both the AccuVote-OS and AccuVote-TSX. The memory card is also used to accumulate and tally election results. Also known as PCMCIA card or “PC Card.”

“Machine ID”

An AccuVote-TX unit is given software tracking number or “Machine ID” during the initial start-up of the AccuVote-TSX in order to track election results by Machine ID at a polling location. This is not the same as the unit serial number.

“Number to Vote For”

The number of candidates, responses or parties that a voter may select in a race without incurring an overvote.

“One Click Vote”

The ability to make an alternative selection on the ballot on the AccuVote-TSX without having to click twice in order to disable an existing selection.

“Official Election Mode”

Official Election Mode is the operating mode in which the official election occurs. This application mode differs from “test mode”, where all administrative functions take place such as machine settings, testing, and diagnostics.

“Overvote”

The condition of voting for more candidates or selections than a race allows. The AccuVote-TSX does not allow a voter to vote for more than the “Vote For” limit of selections. The AccuVote-OS can be programmed to prevent an overvote.

“Party”

The political party affiliation of candidates for federal, state and central committee offices.

“Password”

An authentication of the user’s access to the GEMS, AccuVote-OS, or AccuVote-TSX device.

“PC Card”

Known as PCMCIA card or memory card. Also see “Memory Card”

“PCMCIA Card”

Known as “PC Card” or “Memory Card”. Also see “Memory Card”

“Phone”

The telephone number used for modem transmission.

“Poll Worker Card”

A special smart card programmed with the ability to put the AccuVote-TSX into voter card creation mode or to close the polls and generate totals reports. Also known as “Supervisor Card.”

“Power”

The Power status indicator; defined as either charging (yellow bar on screen) or AC off line which means the AccuVote-TSX is operating off the battery. The AC offline indicator is a red bar that shows the remaining percentage of battery charge available. The AccuVote-OS also indicates when the AC is offline.

“Precinct”

The smallest division of the electorate within a county, city, or district identified by geographic boundaries defined by the local election official. The precinct is expressed either as a base precinct, a geographical unit in which voters vote, or a report precinct, to which election results are reported.

“Programming Election Media”

The act of transferring election and ballot information to election media.

“Protocol”

A set of parameters governing the communication and transfer of information between the host computer and the AccuVote-TSX unit.

“Protection of Results Data”

All results data is protected using standard data encryption methods and by system design functionality. The encryption process makes information indecipherable to protect it from unauthorized viewing, tampering or use.

“Protective Counter”

The total count of all ballots cast on the AccuVote-TSX since the manufacture of the AccuVote-TSX unit. Also known as “System Counter.”

“Provisional Voter Ballot”

Pursuant to Elections Code section 14310, a ballot given to a voter claiming to be properly registered, but whose qualification or entitlement to vote cannot be immediately established upon examination of the index of registration for the precinct or upon examination of the records on file with the county elections official, which includes the list of absent voters.

“Public Counter”

The total number of ballots cast on an AccuVote-TSX during a specific election. Also known as the Election Counter.

“Removable Storage Media”

The external media which stores the election, audit and / or ballot information programmed for the AccuVote-OS and the AccuVote-TSX, and to which election results are tallied once ballots are counted. Also referred to as the Memory Card, PCMCIA card or PC card.

“Recount”

The configuration of an election for recounting one or more races, involving programming selected memory cards and uploading and reporting results for a recount reporting set.

“Report Precinct”

The results of ballots counted in base precincts are tallied to report precincts.

“Rotation”

The candidate rotation rule determines the order candidates are to appear on ballots in a particular geographic area.

“Running State”

In the running, or “Set for Election” state, no modifications are allowed to the election definition. In this state, the removable media is prepared for distribution to the AccuVote-OS and AccuVote-TSX.

“Semi-Official Canvass”

The process of collecting, processing, and tallying ballots and, for statewide elections, reporting results to the Secretary of State on election night. The semi-official canvass may include some or all of the absentee vote totals. The semi-official canvass is contrasted with the official canvass which begins not later than the first Thursday following the election, and for statewide elections shall result in final certification 28 days following the election (Elections Code section 15372)

“Serial Number”

The AccuVote-OS serial number can be located on the back of the unit. The AccuVote-TSX serial number can be found on a label on the external surface of the AccuVote-TSX. This is different from the Machine ID, which is used by the software application.

“Scale %”

The scaling value applied to the AccuVote-TSX image; programmed in GEMS.

“Scale”

The increasing or decreasing of an image from nominal size.

“Straight Party”

A party selected in a straight party or endorsement race which automatically counts candidates endorsed by the party in all straight party-voted races, subject to the straight party tally rule defined for the election. *Straight party voting is not allowed in California.*

“Supervisor Card”

A special smart card programmed with the ability to put the AccuVote-TSX into voter card creation mode or to close the polls and generate totals reports. Also known as “Poll Worker Card”.

“System Total”

The number of ballots cast on the AccuVote-TSX unit since the date of the manufacture of the AccuVote-TSX. It is also referred to as the “Protective Counter”.

“Set-up Diagnostics”

A system test of the software and hardware of the AccuVote-OS and AccuVote-TSX prior to entering ballot logic.

“Smart Card Authentication”

The process by which a Smart Card is inserted into the AccuVote-TSX and parameters verified for the functions being requested. These range from access security to election security to administrative security functions.

“Source Code”

The version of a computer program in which the programmer’s original programming statements are expressed in a source language, which must be compiled, assembled and linked into equivalent machine executable object code, thereby resulting in an executable software program.

“TS Text”

Sets of files residing in GEMS, containing multi-language operational instructions which are programmed to the AccuVote-TSX.

“Type or Network Type”

Type refers to the type of network connection used for transmission; for example, ‘Local Area Network’ if the computer is networked to a hub.

“Undervoted Race”

A race with fewer candidates selected than the number to vote for; cannot occur in a vote-for-one race.

“Unit”

The designated machine number in the Vote Center.

“Upload”

The process of transferring election results from the AccuVote-OS and the AccuVote-TSX units to the GEMS host computer.

“User Name”

The network user ID.

“Version”

The vote center/machine ID download version.

“Visually Impaired Ballot Station (VIBS)”

Visually Impaired Ballot Station (VIBS), an AccuVote-TSX plug-in feature that allows ballots to be voted and cast in audio format.

“Visual Ballot”

The ballot displayed on the touch screen, either when voting a non-VIBS ballot, or when voting a VIBS ballot without the ballot display hidden.

“Vote Center”

A physical polling location, containing one or more voting devices.

“Voted Ballot”

A ballot which has been marked by the voter.

“Votes Cast”

The number of votes cast in a tally, distinct from the number of ballots cast.

“Voting Device”

A Premier ballot counting device; either an AccuVote-OS or AccuVote-TSX.

“Voting Mark”

The mark on a ballot created by the voter’s selection of preferred candidate or measures.

“Voter Access Card”

This card indicates the appropriate ballot to present to the voter and permits an eligible voter to cast a ballot on the AccuVote-TSX. The card will not allow multiple voting or any access to the election management system. Also referred to as a voter “Smart Card”.

“Voter Exit Screen”

The Voter Exit Screen prompts the voter to remove the card from the card reader. When the card is removed, the system returns to the Open Polling Place State.

“Voter Instruction Screen”

The Voter Instruction screen presents the voter with a simple set of instructions for making voter selections and recording the ballot. It appears after the voter inserts the access card.

“Write-In”

Upon choosing the write-in option on the AccuVote-TSX, which allows a voter to select a person whose name does not appear on the ballot, the voter is presented a screen that allows him/her to spell out the name of their candidate by touching the appropriate letters. When the voter touches the Record Write-In button, the name written in appears on the screen showing the applicable contest. The name written in will also appear on the Summary Screen and the AVPM.

The voter can write-in a name on the AccuVote-OS ballot. The voter must fill in the oval next to the write-in name for the vote to count, pending whether the write-in name is a qualified write-in candidate.

Additional definitions may be found in the various User and reference guides that are listed in the appendix

2. Ballot Definition

2.1. Overview

The GEMS ballot layout software is a fully integrated software package. This integrated software is a single program of code that provides for importing of sub-precinct and consolidated precinct information as well as race, candidate and question information from the Election Management system. Information may be entered manually as well. It then is able to lay out the ballot using a fully Windows compliant graphical user interface.

The GEMS system generates the ballots automatically taking the user defined specifics, ie., rotation, font size, ballot definitions and applying them with the touch of a button. Ballots may then be viewed on screen and changed as needed. The many Administrative reports available offer the tools needed for proofing and may be viewed on screen or printed.

2.2. Paper and printing specifications

Ballots printed for the Premier system must conform to unique specifications. These specifications are outlined and in detail in the Premier Ballot Specifications Revision document and as such will be referenced here. They include specifications for paper weight, color, ink and many other items. California EC 13002 specifies that ballots shall be tinted and watermarked or overprinted with a design, to be furnished by the Secretary of State, so that the watermark or overprint shall be plainly discernible.

2.3. Layout requirements and specifications

The Premier system is able to create and tabulate 11 inch, 14 inch or 18 inch paper ballots, portrait or landscape, in a variety of different configurations. GEMS also accommodates the additional languages currently required by law on the paper ballot and is able to have audio ballots in those languages as well. Rotations that are required by California law are easy to select for those races that require them and are easy to rotate.

Ballot layout for the AccuVote-TSX does not require duplicate data entry but uses the information input for the paper ballots and adjusts it for the touch screen ballots. Once created ballots may be modified on screen and the information downloaded easily to the AccuVote-OS or AccuVote-TSX units to proof prior to downloading the memory cards used for the election.

Detailed layout for ballots may be found in the GEMS Election Administrator's Guide. *Managing Ballot Artwork* in the *GEMS 1.18 User's Guide* includes procedures detailing the creation of ballot artwork in GEMS. *Managing Ballot Artwork* in the *GEMS 1.18 Reference Guide* describes the concepts behind the creation of ballot artwork in GEMS.

California EC Div 13, Chapter 3 (13200-13289) contains specific legal requirements for ballots.

3. System Installation and configuration

3.1. Hardware requirements and specifications

The GEMS host computer is used to run the GEMS software, and is configured by Premier. The GEMS server may run Windows 2000 or Windows 2003. The below servers are an example of the servers used to host the GEMS software.

Server Dell PowerEdge 2900 (Tower) and Rack Mount Model 2950

- Dual Core Intel Xeon 5120 4MB Cache (29W18) [222-6451]
- 2GB 533MHz Single Ranked DIMM (2G4D5S) [311-5727]
- Windows Server 2003 R2 5CAL (WSR2S) [420-5796]
- PERC 5/I Integrated Controller (PERC5II) [341-3018]
- Integrated SAS/SATA RAID 5 (MSR5N) [341-2999]
- 73GB SAS 3.5-inch 10K (73A10) [341-3028]
- Tower Chassis Orientation (TOWER) [310-7489]
- Redundant Power Supply with Dual Cords (RPS) [310-7407]
- Tower Bezel (TBEZEL) [313-4363]
- Dual Embedded Broadcom NetXtreme II 5708 Gigabit NIC (OBNIC) [430-1764]
- Broadcom TCP/IP Offload Engine Not Enabled (NTOEKEY) [430-1765]
- Electronic Documentation and OpenManage CD Kit (EDOCS) [310-7402]
- 48X IDE CDRW DVDROM (CDRWDVD) [313-4313]
- 1.44MB Floppy Drive (FD) [341-3053]
- Keyboard, USB (USBK4) [310-8170]
- Two-button USB Mouse (USBMW) [310-8171]
- Dell 22-inch widescreen analog flat panel (E228WFP)
- Soundblaster Audigy 4 sound card

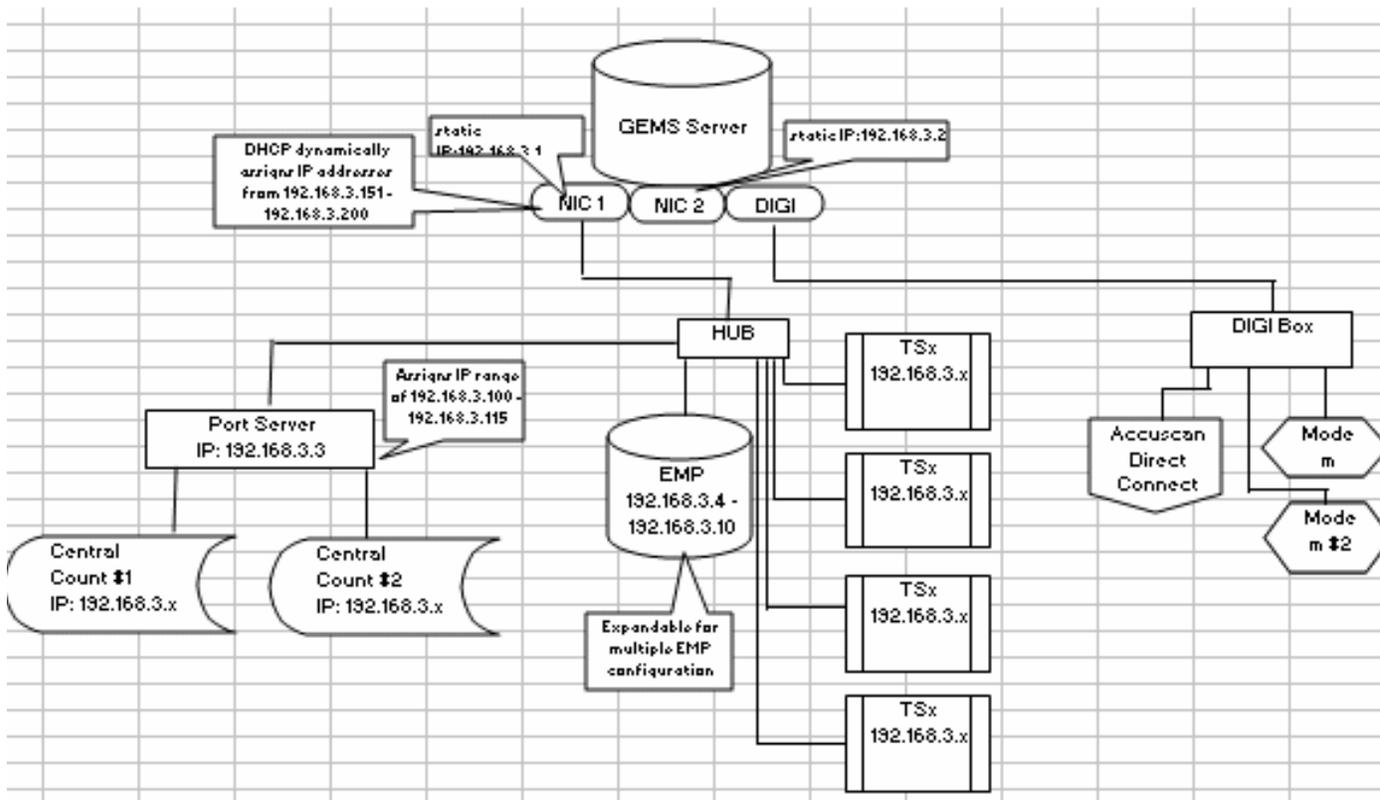
The VCProgrammer and Key Card tool may be run on a small Dell as described above or most often a laptop with a 9-pin serial com port that the smart card burner/reader may be connected.

The following external smart card reader devices may be used with the VCProgrammer and Key Card tool application:

- Securetech ACR-30S
- Securetech ST-100
- AMC Model 152

3.2. Hardware and network setup and configuration

The system is a stand alone closed system, meaning it is not connected to the internet or outside networks. All tabulation peripherals operate independently and are stand alone. The transfer of data is accomplished through closed Local Area Network (LAN) connections and direct connections to the GEMS server. Proper network configuration is essential to efficient and accurate operation and is detailed in each hardware guide. A sample diagram is below and may change according to the actual configuration.



The instructions necessary to configure a Premier GEMS Server are described in the document Windows Configuration Guide and shall be implemented. The instructions are written for a technician who has experience and competency with using the Windows Registry Editor, Windows Administrative Tool, and BIOS setup functions.

The configuration requirements are as follows. Additionally, the Windows Configuration Guide provides additional information on configuring and hardening the GEMS server to prevent malicious attack or tampering. There may be other requirements as needed:

1. All network services and network ports are to be turned off, except those explicitly required to run the GEMS software;
2. the “autorun” feature in Windows is to be disabled;
3. the boot order is to boot from the hard drive only;
4. the BIOS is to be password protected to prevent changes to the boot order.

3.3. Acceptance Testing

Acceptance testing is vital to any system, whether it is a new system or an existing system that has been modified. The procedures for each component of the system have been developed and are included in summary here and in detail in each component hardware guide.

See the system verification in the GEMS Election Administrators guide.

Verify that all of the expected functionality of the GEMS workstation is available. Mark each function on a signoff sheet once it has been verified. The following functions are to be verified:

1. Copy from CD
2. Restore database
3. GEMS version
4. Reports version
5. View card in Card Editor
6. Print ballot artwork
7. Print administrative reports
8. Record/play back audio
9. Download memory card
10. Upload memory card
11. Print results report
12. Perform a backup
13. Review GEMS User's Guide
14. Verify GEMS Read Me file
15. JResult Client version

AccuVote OS Diagnostic Tests

Prior to use in either the central counting mode or precinct counting mode, hardware diagnostic tests shall be performed on every AccuVote-OS to be used in the election. The following diagnostic tests should be performed prior to any election. See the AccuVote-OS Precinct count Users Guide for more information.

To test the various internal components of the AccuVote-OS, go to the diagnostic mode on the AccuVote OS and perform the following:

- a. Verify the operation and setting of the Ballot Box deflector
- b. Verify the setting of the System date and time (consider seasonal time changes)
- c. Test the LCD monitor
- d. Test the System Memory of the AccuVote
- e. Test the operation of internal printer and ribbon
- f. Test the Serial Port on the back of the AccuVote
- g. Test all the scan sensors of the Ballot Reader
- h. Test the memory cards to be used in the election

Diagnostic testing consists of those processes and procedures necessary to ensure hardware to be used in the election is working properly. If malfunctions are encountered, corrections shall be made and recovery procedures implemented. Prior to use, verify and check all cabling and connections for each hardware component are properly attached and connected.

In the event any AccuVote-OS fails after official ballot processing has begun, diagnostic tests must be successfully run on the (failed) component after it has been repaired, replaced, or adjusted (in a manner deemed sufficient by the responsible Election Official and / or designee) to require re-testing for accuracy) before the component is returned to service.

AccuVote-TSX Hardware Diagnostics

Each AccuVote-TSX to be used in an election or as a backup or spare device, needs to pass a standard diagnostic test before placing a removable PCMCIA card in the voting

machine for verification and testing. This allows the jurisdiction's technician to test and or work on the AccuVote-TSX well in advance of having election specific data and the preparation of the removable election media. By conducting diagnostic tests in advance, any hardware and software error condition found can be promptly corrected prior to the election logic and accuracy testing cycle. See the AccuVote-TSX Hardware Guide and Ballot Station User's Guide for more detail and information on the diagnostic testing of the AccuVote-TSX.

Diagnostic testing of the AccuVote-TSX will include verification that all AccuVote-TSX hardware and software components are operational. These components include the audio, serial connectors, date and time, network connection, display, and the printer are functioning in its intended manner.

A historical log of hardware testing and error conditions should be kept by the jurisdiction for all components.

3.4. Software and firmware upgrades

Software upgrades shall be issued to each jurisdiction as directed by the Secretary of State. Firmware upgrades for the AccuVote-OS and AccuVote-TSX may be distributed by the State of California with the written permission of Premier. Installation of these components shall be the responsibility of the jurisdiction, which may or may not request assistance from Premier. Detailed installation instructions and testing are included with each products' user guide. Diagnostic testing should be done after any software and / or firmware upgrade.

Operating system patches and upgrades should be downloaded from a separate computer, copied on a CD and also verified with Premier prior to installation.

4. Election Setup and Definition

Introduction

This section discusses the recommended procedures for programming, proofing testing, transmitting and reporting election results using the Premier voting system. This section breaks down those areas by the GEMS system, and the AccuVote-OS and AccuVote-TSX precinct tabulation systems.

4.1 Global Election Management System (GEMS)

4.1.1 Programming of election management system / software

In California, the following setup is unique in California and should be set up in the GEMS database:

- Disable Bar Code – Under the “AccuVote-TS Option” in GEMS, do not select “Print Bar Codes”;
- Reject Overvoted Races and All Races Blank Voted – Under the “AccuVote-OS Options, Reject Settings” Tab, select the “Overvoted Races” and “All Races Blank Voted” under “Return Ballots With”;
- Using Report 195/196US and Version 1.96 – Under the “AccuVote-OS Options, AccuVote-OS Settings” Tab, select the “195/196US” under “Reports” and select “1.96” under “Version”;
- Do not use characters (e.g., “ % &) in a label, vote center, race or candidate name.

4.1.2 General GEMS Programming Options

Election configuration options are defined under Setup in the GEMS menu bar. Setup options include general administration, users, regions, languages, voter groups, counter groups, ballot and race options, AccuVote-OS and AccuVote-TSX options, reporting sets, monitor scripts and finally, the printer audit function. Refer to Chapter 3 Election Setup in the GEMS User Guide for a more detailed explanation and instructions.

4.1.3 GEMS System Proofing

GEMS System proofing involves verification that the election definition for the specified election is correct, the ballot layout is correct, the hardware is correctly configured and that it correctly tabulates and reports. There should be a checklist to verify all of the proofing steps have been conducted and completed.

System proofing is the in-house review of all election data and the inter-relationships of that data. System proofing shall include, but is not limited to, verification of the correctness of the following:

- Assignment of jurisdictions participating in the election (districts);
- Linkage of precincts to offices in which the election will be held (precincts);
- Ballot content of each ballot type, including offices, district designations,

candidate assignment and rotation, and ballot measures, all in the proper sequence (races and candidates);

- Preparation of instructions, candidates' names, political designations, number to be elected, candidate rotation;
- Verification that all voting precincts have been correctly assigned to a polling location or mail ballot precinct;
- Formatting of headers and footers for each issue and electronic ballot page;
- Printing ballots to verify correctness of content;
- Hardcopy reports produced by the GEMS administrative reporting system should be printed to ensure desired formatting as well as verifying that expected results from testing were transmitted to the GEMS system;
- Ballot facsimiles produced by GEMS;
- Recorded audio files that may be presented to the voter;
- Testing of hardware in the election configuration to verify correct tabulation of paper and electronic ballots;

4.1.4 – GEMS Data Transmission

Transmission to GEMS client devices is managed from the AVServer, Central Count Server, and Regional Server function consoles. All transmissions to and from the AccuVote-TSX, Election Media Processor, AccuVote-OS Precinct Count, and Central Tally System (CTS) are managed from the AVServer function console, while the AccuVote-OS Central Count is managed from the Central Count Server console. These consoles are modal, implying that they may remain active while other GEMS functions may be activated, such as the election results reports windows or the Results Server console.

4.2 AccuVote-OS Testing

Testing of election logic involves both data testing, ensuring the accuracy of cast ballots, and the system testing to ensure that data logic is consistent as it is transmitted from one component of the system to another - as it is downloaded onto memory cards, as ballots are cast, and as results are uploaded to the GEMS host computer application.

Logic and accuracy testing should be conducted on the tabulation memory devices to be used in the election. Diagnostic testing is accomplished on the AccuVote-OS hardware to be used in the election. The diagnostic and logic and accuracy testing may be accomplished independently of each other, as one tests the memory device and the other tests the hardware. The County may choose to do logic and accuracy testing of the memory device and testing of the hardware to be used in the precinct together. However, the hardware and memory devices to be used in the election should be tested as described below.

These procedures could also be used during the post-election logic and accuracy testing process.

4.2.1 AccuVote-OS Diagnostic Testing

AccuVote-OS diagnostic testing should be performed on the AccuVote-OS units prior to each election to test and verify the hardware specifications of the AccuVote-OS unit are functioning in the correct manner.

The AccuVote-OS diagnostic testing is testing the hardware functionality of the AccuVote-OS to verify the unit is operating in the intended manner. This testing includes using various checklists and directions. These items are included in the specific hardware user guides and a detail of the testing is outlined in the GEMS Election Administrator's guide in Chapter 4- Managing the election. These are also available through Premier's representatives

The AccuVote-OS units to be used in an election will have diagnostic tests run. These tests include the following:

- Verifying or setting the AccuVote-OS System Clock for the Election Day time (anticipate any time changes that may occur prior to the date of the election);
- Testing the LCD display;
- Testing the AccuVote-OS System Memory;
- Testing the memory cards to be used in the election;
- Testing and verifying that the printer is working. (This operation prints a test pattern on the tape. This could be saved and attached to an AccuVote unit test sheet, along with other test reports, and saved as part of the election audit trail);
- If the AccuVote-OS is to be used to upload or download memory card data, the serial port should be tested either via a diagnostic test with a serial loop back connector, or by testing the upload or download function of the unit with the GEMS host computer system. Those AccuVote-OS units that are not used for uploading or downloading of data are not required to have the serial connection tested;
- Testing the ballot box "deflector" (the mechanism that sorts ballots in the ballot box);
- Testing the AccuVote-OS, prior to the logic test, by using "diagnostic ballots". These ballots test all read heads on the AccuVote unit and prints a detailed report verifying that all read heads are functional. This test is run on the AccuVote-OS units to be used in the election. The test print out should be attached to the AccuVote unit test sheet, These sheets are kept as part of the testing audit trail and have the date, time, serial number of the AccuVote-OS which produced the tape, and the initials of the person that ran the test.

Once diagnostic testing has been completed on the AccuVote-OS units to be used in the election, the reports indicated above should be attached to an AccuVote-OS testing sheet which shows the serial number of the unit tested. Once diagnostic testing is complete, a test should be done to verify that the logic on the associated memory cards is consistent with the election setup and proofing that has been accomplished for the election.

4.2.2 AccuVote-OS Logic and Accuracy Testing (L&A) Procedures

The logic and accuracy testing consists of those processes and procedures necessary to ensure that the vote tally programs and hardware correctly interpret, summarize and report voters' marks for a specific election. This consists of a series of tests using test ballots which are made from actual printed ballots, or pre-determined test scripts. The results of those tests can be transferred to the GEMS system by transferring results from the memory cards via an AccuVote-OS to GEMS, and from the AccuVote-OS Central Count readers to GEMS.

Successful testing will demonstrate that each candidate and ballot measure receives the proper number of votes. The system reports the proper number of over and under votes, accepts only the proper ballot types and rejects improper ones; and the inactive voting positions are not being tabulated.

The Logic and Accuracy tests, conducted at the time of certification (or re-certification) if necessary to the Secretary of State, storage logs or records, if any, and balancing reports, if any, shall be retained with material for that election for as long as the ballots are required to be kept for the election. (EC §15001 (2005))

4.2.3 AccuVote-OS Logic and Accuracy Testing

Logic and accuracy testing is conducted on the AccuVote-OS and AccuVote-OS Central Count. This testing method ensures the logic of the ballot programming is correct, and the testing reflects the accuracy of the votes cast for each individual oval position tested.

To conduct a logic and accuracy test, logic and accuracy test ballots should be prepared, at a minimum, for each ballot type in the election. These regular official ballots shall be marked "TEST" or otherwise clearly identified as test ballots.

The logic and accuracy test deck is generally made up of "First Oval or Last Oval" ballots for each precinct, LA5, LAn, or LAmx ballot decks, and, if the election has a race where the voter can vote for more than one candidate, multi-vote ballots. The following description of the test decks are recommended procedures should a jurisdiction chose to use the test deck.

- **First Oval / Last Oval** - Test ballots consist of one ballot from every precinct in the election with the first or last oval filled. If the "last" position is a write-in, the deck will have the last position candidate marked in every contest. These will be processed as part of the accuracy test explained in these use procedures. Once the card is run, a result tape can be printed. This tape is kept as part of the election audit. The serial number on which the test was run will be written on the tape, as well as the initials of the person that ran the tape and verified that the first or last candidate correctly received the votes. Finally, the memory cards can be uploaded so that results are verified and confirmed on GEMS. A verification on GEMS can be made to ensure that this test creates 100% precincts counted report.
- **LA5, or LAn, or LAmx Test Deck** - A county may choose to make their own test decks from "blank" ballots ordered from their printer. If a 3rd party printer has been used, this process may be required. Therefore the test deck must reflect a test that checks each candidate position with a known number of votes for each candidate. If the County has a print vendor print the ballots, an automated deck consisting of an LA5, or a specific specified pattern (LAn), or an LAmx deck can be ordered. This deck is made up of election specific ballots that have been marked with a predetermined pattern of votes. For example, an LA5 deck will provide a race with a 1,2,3,4,5 pattern of votes that will be cast for candidates in every contest. For example, the 1st candidate will receive one vote, the 2nd candidate will receive 2 votes, and the 3rd candidate will receive 3 votes and so on until all candidates have had votes cast for them. If there are more than 5 candidates in a contest, the

pattern will repeat so that the 6th candidate will receive 1 vote, the 7th candidate will receive 2 votes and so on until votes have been cast for all candidates.

If there are fewer than 5 candidates, the pattern will only go up to the highest number of candidates in that race. At a minimum, this deck is created for at least one precinct in each ballot style, or as determined by the Election Official. When an LA5, “n”, or max test ballot deck is run for each ballot style, a “first or last” oval deck should also be run for all remaining precincts to verify that all precincts are tested for proper printing of precinct ID marks on each ballot and that the appropriate “precincts counted” numbers are achieved.

The purpose of any of these L&A decks is to test that all candidates and races on all ballot styles are counting correctly. After each L&A deck is processed thru the AccuVote-OS unit in precinct or central count mode, a precinct report can be generated to verify that the correct votes are being tabulated by the AccuVote-OS unit and/or by GEMS in the case of central count AV or mail precincts.

It is recommended that as many L&A decks be used as is reasonable for the election, given the time and resources available. However, at a minimum, the L&A deck must be run for every ballot style. For example, an even year primary may preclude a county from running an LA5 (or other L&A) deck for every precinct due to the number of ballot styles and parties in an election.

For primary elections, an L&A deck should be created for each of the parties in a precinct ballot style.

When using the automated L&A test decks, it may be noted that for offices that rotate across districts, an Election Summary Report on GEMS may not maintain the 1,2,3,4,5, etc. pattern. In this case a report should be printed so that individual precincts may be viewed with results isolated for each candidate and race, thereby clearly showing the expected pattern of votes within each race.

- **Multi-vote test deck:** This test deck is produced by a print vendor’s automated test deck process. Where a county is using a certified printer to print the AccuVote optical scan ballots, the county will need to prepare its own test decks to test for “vote for more than one” races to confirm that it is programmed for more than one candidate. This deck is produced for Ballot Styles where multiple votes (Vote For Two or more) are authorized. All races that are “Vote for one” are ignored in this deck. The first ballot is the “overvote” ballot. Each race has one more prefilled oval than allowed for the race. The next set of ballots rotate in combinations of the number of votes allowed, e.g. with Vote for Three and 6 candidates, the deck would produce a ballot for ovals 1,2,3 followed by 2,3,4, then 3,4,5, and then 4,5,6; continuing on to the last oval in the race. Tabulation would be 1 vote for first and last candidate, 2 votes for 2nd and 2nd from last, 3 votes to the 3rd and 3rd from last and so on until the candidates in the middle are receiving the maximum number of votes allowed.

A logic and accuracy test should be performed on the AccuVote-OS units and the Central Count readers as applicable. A precinct results tape should be printed for

each logic test on the AccuVote-OS units. This tape should show the expected pattern of votes for each candidate race based on the test deck created by the County, or ordered from the ballot printer. As the AccuVote-OS units is tested, it should be verified for the expected results, uploaded to GEMS, and reports printed that are confirmed to have identical results to the precinct results tapes printed during the test. A recommended process for conducting a logic and accuracy test on the AccuVote-OS unit follows:

- Run an LA5 (n, or max) deck for every style that will be used for the AccuVote-OS precinct count and central count;
- Run a First Oval / Last Oval deck for all precinct not included in the LA5 (n, or max) decks;
- Print the reports for the AccuVote-OS and examine for expected results pattern;
- Upload the memory cards to the GEMS system;
- Once the memory cards have been loaded with test data, the memory cards should be uploaded to the GEMS host. After all memory cards have been uploaded, a GEMS Summary Report, a specific precinct report or a Statement of Votes Cast (SOVC) should be printed and used to compare the results received by GEMS with the precinct tapes printed during the L&A test deck or “first or last” oval deck runs of the AccuVote-OS unit.

4.3 AccuVote-TSX Testing

Testing of election logic involves both data testing - ensuring accuracy of cast ballots, and system testing to ensure that data logic is consistent as it is transmitted from one component of the system to another - as it is downloaded onto memory cards, as ballots are cast, and as results are uploaded to the GEMS host computer application.

These procedures could also be used during the post-election logic and accuracy testing process.

4.3.1 AccuVote-TSX Diagnostic Testing

AccuVote-TSX diagnostic and accuracy testing should be performed on the AccuVote-TSX units prior to each election to test and verify the hardware and software specifications of the AccuVote-TSX unit are functioning in the correct manner.

The AccuVote-TSX diagnostic testing is testing the hardware and software functionality of the AccuVote-TSX to verify the unit is operating in the intended manner. This testing includes using various checklists and directions. These items are included in the specific hardware user guides as well as through Premier’s representatives.

The AccuVote-TSX units to be used in an election include the following:

- Verifying or setting the AccuVote-TSX System Clock for the Election Day time (anticipate any time changes that may occur prior to the date of the election);
- Testing the AccuVote-TSX Card Reader;
- Testing the AccuVote-TSX Serial Port;
- Testing the AccuVote-TSX Audio;

- Testing and verifying the touch screen is accurately recording a selection on the screen;
- Testing the memory cards to be used in the election;
- Testing and verifying that the printer is working.

Any hardware failure of a component during testing will necessitate re-testing of that hardware with election specific data prior to placing that hardware back in use for the election.

Once diagnostic testing has been completed on the AccuVote-TSX units to be used in the election, the AccuVote-TSX testing sheet should be recorded and signed by the authorized county tester and stored. Following the diagnostic test, a logic and accuracy test should be done to verify that the logic and accuracy on the AccuVote-TSX unit is consistent with the election setup and proofing that has been accomplished for the election.

4.3.2 AccuVote-TSX Logic and Accuracy Testing Procedures

The logic and accuracy testing consists of those processes and procedures necessary to ensure that the vote tally programs and hardware correctly interpret, summarize and report voters' marks for a specific election. This consists of a series of tests using test ballots or pre-determined test scripts. The results of those tests can be transferred to the GEMS system by transferring results from the memory cards via an AccuVote-TSX to GEMS.

Successful testing will demonstrate that each candidate and ballot measure receives the proper number of votes. The system reports the proper number of over and under votes, accepts only the proper ballot types and rejects improper ones; and the inactive voting positions are not being tabulated.

The following are some recommended procedures for the logic and accuracy test for the AccuVote-TSX:

The logic and accuracy tests will be conducted using test materials in such a manner as to meet these guidelines. All tests shall result in reporting that matches predetermined results. All reports and test materials must be retained as part of the official election record for the time period dictated by law. [EC §15001(c)(1)];

The Logic and Accuracy tests, conducted at the time of certification (or re-certification) if necessary to the Secretary of State, storage logs or records, if any, and balancing reports, if any, shall be retained with the election material as long as the electronic ballots are required to be kept for the election. (EC §15001 (2005));

The responsible elections official or authorized designee shall prepare the logic and accuracy test ballot decks or scripts and make it available for testing. The results reports of the logic and accuracy tests must be available for inspection and sign off by the county elections official and / or the authorized designee;

The logic and accuracy testing for the AccuVote-TSX and the AVPM audit trail should include the following considerations to represent and simulate an election environment:

- Testers should vote to simulate actual election conditions;
- The election test script should have a random sample of precincts for the election. For a primary election, the parties, including the “crossover” parties, were applicable as well as each unique style should be included;
- The test script should test for write-ins, undervotes, blank votes and a number of blank ballots;
- The testing should include the printing of the AVPM audit trail to test the accuracy of the audit trail;
- The AVPM audit trail should be verified against the AccuVote-TSX results report and the GEMS results report.

The election administrator or authorized designee should enter the voted selections, and cast the votes in a predetermined voting pattern. The voting pattern should insure each candidate and each ballot measure receives at least one vote. The test should include at least one under vote (it is not possible to over vote on the AccuVote-TSX) and accepts only the proper ballot types.

The resulting logic and accuracy vote tallies shall be compared in detail with the predetermined logic and accuracy vote tallies. Any differences between the two logic vote tallies needs to be resolved, and logic and accuracy testing shall be performed as many times as may be necessary to achieve a logic and accuracy vote tally identical to the predetermined logic vote tally.

If the results report shows any variance in the tabulation of votes, the cause for the error shall be ascertained and corrected and an errorless count shall be made before the system is approved for use in counting votes. Pre-conditions for performance of tests, including test decks.

4.3.3 AccuVote-TSX Logic and Accuracy Testing

The logic and accuracy test is an essential method of testing electronic ballots to be used in that particular election, ensuring that the AccuVote-TSX units perform properly. The purpose of this test is to ensure that the ballot used with a particular election will function properly when run with the ballot tabulation software for that election.

The tests may be conducted by using a combination of automated and manual tests that incorporate pre-determined test scripts to verify that the system is correctly and accurately recording, tabulating, and reporting vote results. These tests which may be conducted are:

- a. An automated test script which provides a unique vote value for all candidates within a race, and tests all ballot styles and rotations in the election. This data is uploaded to GEMS. The summary report from the AccuVote-TSX is then compared with the Summary Report of the GEMS server to ensure that tabulation and reporting of candidate votes in all races is occurring accurately on both systems. A report is used to verify that the results are identical at the precinct level.

This process tests the reporting functions of GEMS and the AccuVote-TSX as well as providing verification that the election logic is mapped correctly between the GEMS server and the AccuVote-TSX ballot styles in the precincts;

- b. An automated test process which gives votes to all candidates in all precincts. This test verifies that all precincts and races are correctly mapped between the GEMS database and the AccuVote-TSX ballot station;
- c. Use of one of two possible manual vote tests: A manual testing process, which incorporates a pre-determined random script of votes for all races and ballot styles as described below, or a manual testing process, aided by the testing software, which provides a manual vote for each candidate in each ballot style of the election, but provides a unique value to all candidates within a race. Votes will be checked in GEMS to determine the logic and accuracy;
- d. Another test following the manual or automated logic and accuracy test is to print the ballots on the AccuVote-Printer Module (AVPM) during this process so that the AVPM testing occurs for races and ballot styles for that election. These printouts become part of the audit trail which shows that the AccuVote-TSX hardware and software are accurately recording and printing ballots as voted for all candidate and race combinations.

If a voting machine or the central tabulating system does not accurately count the test script or test vote, the cause for the error shall be ascertained and corrected. An errorless count shall be successfully produced before the system is approved for use in counting votes.

4.4 AccuVote-OS and AccuVote-TSX Audit Log Retention

The GEMS Audit log contains a complete record of all transactions that have occurred in the election in GEMS, ordered by date and time. These should be printed and retained as part of the official election. This log is located in the drop down list under the GEMS menu.

Specific transaction in the AccuVote-OS Precinct Count is recorded to the Audit Log, which is stored on the memory card. The Audit Log can neither be deleted or altered other than by means of the automatic posting of event transactions to the log. The audit log will be printed out at the end of Election Day and posted.

All system operations performed on the AccuVote-TSX unit are logged to the unit's System Log. All election related operations are logged to the Audit Log. When an installed memory card has been programmed with election data, system operations are logged to both the Audit Log and the System Log. The Audit Log is stored on the memory card and the unit, and the System Log is stored on the unit only.

As with the GEMS System logs, the hardware audit logs should be printed and retained as part of the official election. Please refer to the Ballot Station User Guide and the AccuVote-OS precinct count user guide for more detail.

4.5 Public Logic and Accuracy Board and certification of testing

The jurisdiction may appoint a Logic and Accuracy Board to oversee the public logic and accuracy testing. The public logic and accuracy board shall be appointed by the responsible election official or by the authorized designee. The Counties are responsible for the development of its Logic and Accuracy Board.

4.6 Ballot tally programs

A copy of the ballot tally program used for the election shall be sent to the Secretary of State prior to each statewide election in the timeframe prescribed by law [EC§15001(a) (2005)]. Any subsequent changes to the ballot programs must be resubmitted to the State.

4.7 Election Observer Panel

All procedures prescribed in this procedures manual should be carried out in full view of the public insofar as feasible. In addition, the responsible elections official shall devise a plan, subject to the approval of the Voting Systems Panel, whereby all critical procedures of the vote tallying process described in this procedures manual are open to observation by an Election Observer Panel. Representatives of the qualified political parties and representatives of the news media shall be among those invited to serve on this Panel and shall be given the opportunity to observe that the correct procedures have been followed in the receiving, processing, and tallying of all the voted ballots. The Election Official shall appoint an Election Observer Panel; failure of any or all invited parties to participate on the Panel shall not stop procedures from continuing as otherwise required by law.

4.8 Hardware maintenance and preparation for use

The ballot counting equipment must be maintained in a satisfactory manner in accordance with vendor specifications, where available. Each individual component testing and maintenance if necessary shall be performed by the authorized personnel that have been trained to do this before each election.

Any equipment, or component, that fails or malfunctions during maintenance and testing shall be serviced, repaired, or replaced and appropriately tested prior to the use of that equipment or component in any election. All equipment and specialized vote tabulating equipment must be certified for use in elections by the Secretary of State prior to use in any election.

Additionally, all equipment to be used in each election should be maintained at all times in good working order and all appropriate maintenance and other applicable logs should be kept for each piece of the system.

For each statewide election, the responsible county elections official should prepare a list, including quantities, of all equipment to be used to tabulate votes during the semi-official and official canvass.

Seven days before each statewide election, the elections official shall certify to the Secretary of State the results of the logic and accuracy tests as well as the accurate functioning of all ballot counting equipment. This certification shall also affirm the use of the same equipment for pre-election testing and for semi-official and official vote canvasses. In the event of a change to the ballot tally program occurring after this

certification, an amended certificate shall be submitted no later than the day before the election. EC §15001(a) (2005)]

In the event any of the host tabulation computer equipment is repaired, altered or replaced following the certification specified in the above section and prior to completion of the official canvass of the vote, an amended certification of logic and accuracy testing and a revised list of equipment used must be submitted to the Secretary of State not later than submission of official canvass results.

5 Polling Place Procedures

5.1 Precinct supplies, delivery and inspection

Precinct Supplies

In addition to those supplies required for the conduct of elections generally, the Election Official shall supply to each precinct a sufficient quantity of the following:

For AccuVote optical scan precincts

- a. Marking devices compatible with the AccuVote-OS Voting System as recommended by Premier.
- b. Ballots of such form as required for tallying by GEMS or the Vote Tally System. In primary elections, ballots shall be appropriately tinted or otherwise identified for each political party and for nonpartisan voters, as directed by the Secretary of State.
- c. Secrecy envelopes or folders in sufficient quantity to conduct the election. These envelope/folders must entirely cover the ballot area on which voting marks are made. The envelopes/folders provide security coverage of voted ballots until the ballots are deposited into the ballot box. The envelopes/folders are not deposited in the ballot box with the voted ballots, and may be reused by successive voters.
- d. One or more ballot boxes or containers that may be sealed or locked, into which is placed each voter's ballot(s).
- e. Containers or envelopes in which to enclose the following: (1) election supplies; (2) voted ballots; (3) provisional, voted absentee, spoiled, unused and cancelled ballots. At the option of the Election Official, the container provided in Item d may be used for all or part of this requirement.
- f. A Precinct Ballot Statement.
- g. Other forms, logs, and seals for containers, equipment and supplies necessary for the conduct of the election.

For AccuVote-TSX precincts

- a. AccuVote-TSX with AVPM including sealed canister and paper roll.
- b. Keys to open the PCMCIA door and printer compartment.
- c. Voter card encoders with backups.
- d. Voter access cards 3 if only one unit, 10 if more than one.
- e. AccuVote-TSX units may be used as backup Voter Card encoders.
- f. Additional AVPM units to use as backups if needed.
- g. Additional security canisters, seals and paper rolls (1 per AccuVote-TSX).

- h. Privacy screens.
- i. Demonstrator unit if available.

5.2 Polling Place Setup

For the AccuVote-OS

The precinct officer shall check that the following has been delivered and verified:

- a. An AccuVote-OS tabulator with the correct memory card installed. This can be verified by inspecting the printed Results Tape. If Multiple Precinct Processing is to be implemented, the AccuVote-OS device shall be located so that it is equally accessible to voters and precinct officers of each precinct.
- b. A ballot box compatible with the AccuVote-OS. It has three compartments or bins with slots. During operation, the AccuVote-OS is inserted into the top of this ballot box, and processed ballots emerging from the AccuVote-OS are fed into the right and center bins.
- c. Two keys appropriately labeled. One key will open the printer compartment on top of the AccuVote-OS. Another key will open all the doors of the ballot box.
- d. On receipt of the AccuVote-OS, verify that the identification number on the AccuVote-OS is the same number that is listed on the Voting Device Report or precinct supply list. The serial number is located on the back of the AccuVote-OS next to the plug.
- e. Check the number on the seal that locks the memory card slot in place. This is the same number that is listed on Voting Device Report or precinct supply list. Report any irregularity (broken seal, incorrect seal) to the Election Official. Voting may commence, but ballots are to be deposited in the left side auxiliary bin until corrective action, if any, is taken or directed by the Election Official.

AccuVote-OS Ballot Box set up

- a. Verify that no ballots remain in any of the ballot box bins from testing or previous elections. Invite any persons assembled at the polling place to view the empty ballot box and observe the closing of the ballot box;
- b. Remove the ballot slot cover on top of the ballot box;
- c. Lift the AccuVote-OS and slide it into place on the top of the ballot box, leaving enough room in the back of the unit to turn the power switch on. Thread the power cord through the chute in the ballot box and plug it into the back of the AccuVote-OS unit;
- d. Push the AccuVote-OS back against the ballot box plug. Lock the front door of the ballot box to firmly secure the AccuVote-OS to the ballot box;
- e. Close and lock all ballot box doors. The auxiliary bin door may be left open.

For the AccuVote-TSX

To set up the AccuVote-TSX with the AVPM refer to the AccuVote-TSX Poll workers Guide and complete the following steps:

- a. Assemble voting booths with AccuVote-TSX;
- b. Install AVPM, feed paper and load security canister. The poll workers will be given instructions on the assembling of the AVPM to the AccuVote-TSX;
- c. Plug the AccuVote-TSX into the AC outlet;
- d. Unlock side door and power on;
- e. Verify that the serial number and precinct on the security canister and the display screen match with one another. Verify the chain-of-custody log is correct. If there is a discrepancy, contact the county help desk to report the discrepancy;
- f. Report any problems to the appropriate election official / jurisdiction hotline and / or help desk;
- g. Make a demonstrator device available, if applicable.

5.3 Opening the polls

For the AccuVote-TSX

To open the polls with the AccuVote-TSX:

- a. Perform a printer test to verify the printer is working;
- b. Allow a zero report to print, and designate the authorized election officials to verify the zero counts in all races and sign in appropriate space on the tape;
- c. Start the take up spool on the AVPM to the canister where it will be stored;
- d. Lock the printer compartment and side door;
- e. Place key in envelope for storing while the polls are open;
- f. Before the precinct board allows votes to be cast on any machine, it shall proclaim aloud at the place of election that the polls are open.

For the AccuVote-OS

To open the polls with the AccuVote optical scan precincts:

- a. Unlock the printer cover and turn the AccuVote-OS on;
- b. The AccuVote-OS will automatically print the Zero Tape report when it is turned "ON";

- c. Check the AccuVote-OS Liquid Crystal Display (LCD). The LCD indicates the poll number and the public counter are at 0. If the LCD display shows any number other than "0", turn off the unit and call the county help desk for further instruction;
- d. The Zero Tape is the final initialization report that shows no ballots have been counted. Depending on how the election memory card is programmed, it may also show zero vote totals for each race and measure;
- e. If the Zero Tape does not automatically print when the AccuVote-OS is turned on, report the issue to the Election official. Voting may commence, but ballots are to be deposited in the left auxiliary bin until corrective action is taken;
- f. Verify that all candidate names and propositions displayed on the Results Tape are the same as they appear on the official ballot;
- g. Verify that all candidate names and propositions have a zero total;
- h. If any of the conditions described under "e" or "f" do not exist, this must be reported to the Election Official. Voting may commence, but ballots are to be deposited in the left auxiliary bin until corrective action is taken;
- i. The precinct board shall sign the zero tape. The zero tape is not detached. Invite any persons assembled at the polling place to view the zero tape. Roll or fold tape and lay the zero tape inside the AccuVote-OS. Replace and lock the printer cover. The AccuVote-OS is ready to accept ballots.

5.4 Polling place procedures

The following are recommended polling place procedures for the AccuVote-OS and the AccuVote-TSX units:

For the AccuVote-OS

- a. Surrender of Absentee Voter Ballot: No person to whom an absent voter ballot was issued is permitted to vote at the polling place unless he or she surrenders the absentee ballot. The ballot is to be marked "SURRENDERED" and placed in the container marked for spoiled and unused ballots. The voter is then permitted to vote in the normal method for the precinct. If the voter cannot surrender the absentee ballot, that voter may be issued a provisional ballot.
- b. Voted Ballot Sealed: If a voter returns a voted absentee ballot, verify that the ballot is sealed and that the signature of the voter is on the identification envelope.
- c. During the day, at least every hour, inspect the AccuVote-OS to ensure that the power cord is connected and screen is displayed properly.
- d. Offer instructions to voters in the proper method of inserting a voted ballot into the AccuVote-OS.

For the AccuVote-TSX

- a. Surrender of Absentee Voter Ballot: No person to whom an absent voter ballot was issued is permitted to vote at the polling place unless he or she surrenders the absentee ballot. The ballot is to be marked "SURRENDERED" and placed in the container marked for spoiled and unused ballots. The voter is then permitted to vote in the normal method for the precinct. If the voter cannot surrender the absentee ballot, that voter may be issued a provisional ballot.
- b. Voted Ballot Sealed: If a voter returns a voted absentee ballot, verify that the ballot is sealed and that the signature of the voter is on the identification envelope.
- c. The poll worker, once verifying the voter on the polling roster, is precluded from notating the date and time the voter has voted on a device.
- d. After the voter's name is checked off the roster, they will be given a Voter Access Card. A voter access card is created using either a AccuVote-TSX, Voter Card encoder, or VCProgrammer. A voter will be provided instructions on using the AccuVote-TSX.
- e. The voter inserts the voter access card into the AccuVote TSX, and the system reads the voter access card for the appropriate ballot display.
- f. The voter selects the ballot choices and reviews those choices on the AccuVote-TSX summary screen.
- g. The AVPM audit paper trail will generate a paper summary of their ballot selection to verify against the on-screen summary of the ballot. The voter has the ability to accept or reject the on-screen summary.
- h. Upon casting the vote, the AVPM paper audit trail results are stored on both the removable media and the flash memory. The AVPM audit trail is automatically taken up into the security canister.
- i. After touching the "Cast Ballot" button, the public counter and protective counter is incremented. Redundancy provides a check and balance where the numerical count of both files must match.
- j. The electronic results are stored electronically in a random order.
- k. After recording the ballot, the voter access card is disabled.
- l. Whenever the system is in use, the audit log is activated.
- m. Upon completion of all audit checks, the next voter is allowed to proceed with making selections and casting his/her ballot.

AccuVote-TSX Privacy

The county elections office will endeavor to arrange the AccuVote-TSX units, wherever and whenever possible to provide voters with a private voting environment.

In jurisdictions where the main voting method is paper and the AccuVote-TSX is used only for ADA accessibility, the poll workers may allow non-ADA voters to vote on the AccuVote-TSX to provide additional votes and paper audit trails to the AVPM and to guarantee anonymity for the voters.

When a blind voter is using the AccuVote-TSX, the poll worker or blind voter's assistant shall place the VIBS cover on the AVPM printer housing. The VIBS cover and the blank AccuVote-TSX screen will provide the blind voter privacy when using the AccuVote-TSX in VIBS mode. The Voter may be assisted with inserting the Voter Access card if necessary as well.

Voters should be given a large magnifier, if needed, to magnify and see the contents of the AVPM window.

Voters who leave the booth without printing their ballot or casting their ballot ("Fleeing Voter") will have their voter access card ejected and their vote not counted. There is a 30 second time out message that will appear on the screen after a period of 2 minutes of inactivity. The screen will count down from 30 seconds, and will allow the voter to resume voting by pressing the "resume" button, or the countdown will continue to 0, at which time the voter access card is ejected and the ballot is cancelled.

If the voter allows the AccuVote-TSX to time out, a new voter access card will need to be coded.

For the AccuVote-OS

- a. The poll worker, once verifying the voter on the polling roster, is precluded from notating the date and time the voter has voted on a device.
- b. Instruct each voter in the proper method of voting by filling in the oval, casting write-in votes and using the secrecy sleeve. Each voter shall be given further instruction and practice time with a demonstration ballot, if necessary.
- c. Write-in space is provided on the ballot. The voter must both write the name of the candidate and fill in the voting position oval for the vote to be counted by the AccuVote-OS.
- d. Instructions in inserting voted ballots into the AccuVote-OS shall be given after the voter has completed voting, if necessary.
- e. Check periodically to make sure the AccuVote-OS is working properly.

Left Side Auxiliary Bin of the AccuVote-OS

The Left Side Auxiliary Bin of the ballot box may be used as a storage area, if none has been provided, for the temporary storage throughout Election Day for these ballots:

- Delivered, voted Absentee Ballots;
- Surrendered Absentee Ballots, unless directed otherwise by the Election Official;
- Voted Provisional Ballots;

- Voted Ballots that will not be accepted by the reader;
- Ballots voted during emergency periods.

During the time when the polling place is open, the results tape shall not be removed, nor shall any portion of the results tape be torn off.

If for any reason the AccuVote-OS becomes inoperative, voting will continue. From the time the device becomes inoperative, until is the AccuVote-OS is made operable or replaced, voted ballots shall be placed in the Left Side Auxiliary Bin. If, and when the AccuVote-OS is restored to operation, a precinct officer, if approved by the election official or authorized designee, witnessed by a second precinct officer shall enter ballots, which have been stored temporarily in the Left Side Auxiliary Bin, into the AccuVote-OS.

This process shall neither hinder nor delay voting, and shall be performed during inactive voting periods, or after the last voter has voted and before the “Ender Card” is processed. During this process, if a damaged ballot is encountered, it shall be placed in an envelope or container appropriately labeled. Such ballots shall be held by the Election Official for inclusion in the Final Official Canvass.

5.5 Special needs voters

For AccuVote-TSX Precincts – Voter Assistance

In a polling location where there is only one AccuVote TSX, it is advisable that the poll workers encourage other voters to use the AccuVote-TSX unit in order to protect anonymity.

The AccuVote-TSX VIBS is designed for use by voters with a wide variety of disabilities.

A precinct officer shall be available for assisting voters on the AccuVote-TSX device. For those voters with disabilities, the poll worker can assist in adjusting the angle for the AccuVote-TSX for the voter prior to the voting process. Additionally, the voter has the option of selecting a high contrast screen, or the large font screen to enhance the text.

For a blind voter, the VIBS kit can be used to provide audio functionality. The audio is played for them to make their selections. With the option to have the screen completely blank to ensure their privacy even with an assistant standing near by, blind voters are able to listen to an audio ballot and make their selections with the keypad. The 5 key, with its raised dot, is used to select and de-select races and candidates when their names are read.

Voters with Limited Dexterity may use the tethered keypad on the AccuVote-TSX which can be placed in their lap for use without the need to raise their arms. The adjustable screen angle enables them to position themselves close to the touch screen. The voter could also utilize a mouth stick to touch the screen.

For AccuVote-OS Precincts – Voter Assistance

A precinct officer shall be available near the AccuVote-OS device for assisting voters. Secrecy sleeves should be utilized to protect the voter’s privacy. This officer may be on the board of any precinct, if Multiple Precinct Processing is implemented. The same officer does not necessary need to perform these duties throughout the day. Those duties may be rotated between each precinct.

- a. Make sure the voter stub has been removed from the ballot and given to the voter. Assist the voter, if requested, in how to insert his/her ballot. An Assisted Voter affidavit

does not need to be completed unless the assistance requires the viewing of the voting positions on the voter's ballot.

- b. Read and inform the voter of the text of messages displayed by the LCD, if any.
- c. Inform the voter of what corrective action, if any, may or must be taken, or inform the voter of what options, if any, may or must be chosen.
- d. When assisting the voter as described above, the precinct officer shall position him / herself, so that the voted portion of the ballot shall not be in that officer's view.

5.6 Provisional voters

For the AccuVote-TSX

The AccuVote-TSX (DRE) Ballot Station is capable of separating provisional ballots from non-provisional ballots. When a voter appears at the precinct and is identified as a provisional voter, the AccuVote-TSX ballot station software identifies the voter's ballot, so that it can be retrieved, should the voter be determined eligible or ineligible by the canvassing board. In order for that ballot to be retrievable, the provisional voter is processed and assigned a voter ID number. The voter's provisional ID number is stored in the voter access card by the poll worker along with the voter's precinct and ballot style information. The voter proceeds to the AccuVote-TSX Ballot Station, inserts the voter access card, votes and casts the ballot, and returns the voter access card for re-use by the polling place.

The provisional ballot is recorded but not added to the result totals. Should the provisional voter's ballot be determined to be eligible for counting by the Election Board during the post election canvass, it would be identified in the election system by the provisional voter's ID number, and retrieved and added to the election result totals. This process is accomplished in GEMS on the challenged ballot screen, where the provisional voter's ID number is located. The GEMS administrator has the option to "accept" or "reject" the provisional ballot.

When electronic provisional (challenge) voter ballots are used, they will be identical in form as official electronic ballots. In lieu of electronic provisional ballots, paper provisional ballots may also be allowed. Provisional voter ballots are to be used at all elections by voters who claim to be registered but whose right to vote cannot be immediately established. If a voter's eligibility to vote cannot be established, the election official uses the Voter Card Encoder to designate the provisional (challenge) voter and load the applicable ballot, and the provisional voter's results will then be automatically isolated by the AccuVote-TSX system for resolution after the election. Procedures should be established to reconcile, count and / or reject the appropriate Provisional ballots cast electronically; these procedures should be in place for Paper Provisional ballots as well.

For the AccuVote-OS

Paper provisional ballots may be issued at the polls according to the prescribed state laws. The procedures for issuing a paper provisional ballot are the same as an AccuVote-TSX precinct in that the provisional voter will be assigned a provisional ID number. The provisional ID number will be on the voter's provisional ballot envelope. The provisional ballot will be adjudicated during the post election canvass process by a jurisdiction's canvass board, or by authorized members of the jurisdiction's staff.

5.7 Closing the polls and vote reporting

For the AccuVote-OS

Closing the polls shall be conducted as prescribed in Election Code Section 14401 et. seq.

The Following Procedure must be completed in Public View:

1. Promptly at 8 p.m. declare, "The polls are closed". Any voter in line at the time of closing must be allowed to vote. No voter who arrives after 8 p.m. may vote.
2. Precinct voter ballots: The AccuVote-OS will have a total number of ballots counted on the Results Tape. Keep the ballots with the write-in votes separate from other ballots.
3. Process Voted Ballots: All ballots cast at the polls and counted through the AccuVote-OS in the precinct are counted, except for the write-in votes. All of the cast ballots should be reviewed for valid write-ins. Upon inspection, if there are write-in vote(s), no further action is required. Place the ballot cards with write-in votes within a precinct in one stack.

Ending the Election

Following the close of the polls, the precinct board shall remove any and all voted ballots from the Left Side Auxiliary Bin that were not counted by the AccuVote-OS. The precinct board may attempt to feed these ballots into the AccuVote-OS for counting, or return those ballots to the central election office for processing. Those ballots that continue to be rejected by the AccuVote-OS should be placed inside the designated container as directed by the Election Official and sealed.

The precinct board shall unlock and remove the printer cover of the AccuVote-OS device, then obtain access to the front of the AccuVote-OS by unlocking the top front door of the ballot box. While holding the YES and NO button on the front of the AccuVote-OS at the same time, insert the Ender Card into the AccuVote-OS. This will initiate the FINAL Results Tape that will print automatically. If the tape does not print, call the Election Official immediately. The printed tape will include both the ZERO TOTALS TAPE and the FINAL RESULTS TAPE. The precinct board shall tear the tape from the AccuVote-OS and return it to the Election Official as specified.

The precinct official shall print two copies of the audit log and two copies of the election summary report from the AccuVote-OS and post one copy of each report at the polling place. The other copies shall be returned to the central elections office. The poll workers must sign the reports. The precinct board also records the ballots cast total on the Precinct Ballot Statement as directed by the Election Official.

After printing the final results tape, the precinct board returns the AccuVote-OS memory cards to the Election Central for direct upload to the GEMS Server. THE MEMORY CARD SHALL NOT BE REMOVED FROM THE ACCUVOTE-OS UNIT EXCEPT BY AN AUTHORIZED ELECTION OFFICIAL which may include poll workers, county officials and couriers. There shall be two people transporting the memory cards from the precincts to the accumulation center / election office at all times.

Examine the Ballot Bins: Any delivered voted absentee ballots shall be placed in the designated container provided for that purpose. Place any surrendered absentee ballots in the designated container provided for that purpose. Place any voted provisional ballots in the container provided for that purpose.

The Precinct Board will remove all of the voted ballots from the ballot box. The Precinct Board will place voted ballots into envelopes or containers and seal with the seal provided for that precinct. Also, the write-in ballots from the center compartment of the ballot box will be removed and place in an envelope or container as directed by the Election Official.

For the AccuVote-TSX

The Following Procedure must be completed in Public View:

Promptly at 8 p.m. declare, "The polls are closed". Any voter in line at the time of closing must be allowed to vote. No voter who arrives after 8 PM may vote.

Ending the Election

- On all AccuVote-TSX units, insert the Supervisor card.
- At the supervisor screen, enter the assigned Personal Identification Number to enter the supervisor screen, and then press the "OK" button.
- Press the End Election button.
- Open all AVPM units with the AVPM key and follow the county procedures for printing the report tapes. Poll workers are not allowed to break the security seal on the AVPM security canister and remove the tape housed within the AVPM security canister.
- At the report prompts, press the print buttons according to poll worker instructions. Print two copies of the audit log and two copies of the election summary report from the AccuVote-TSX and post one copy of each report at the polling place. The other copies shall be returned to the central elections office. The poll workers must sign the reports.
- At the prompt, use the key to open the side cover on all units (remove transport media if election is ending) and turn the AccuVote-TSX power off. Unplug the AccuVote-TSX and close the booth.
- If necessary, follow the county procedures for upload accumulation.
- Seal the PCMCIA card(s) in the designated envelope for transport. Count to make sure there is a PCMCIA card for each AccuVote-TSX Ballot Station. There shall be two people transporting the memory cards from the precincts to the accumulation center / election office at all times.
- Collect any absentee voter ballots or paper provisional voted ballots, if used.
- Complete all relevant paperwork as required by the jurisdiction and seal in appropriate containers for return to Election Central.

Packaging for Return

- Package AVPM security canisters as directed by the Elections Official.
- Package AVPM printer housing and paper roll as directed by the Elections Official.
- Package or seal all other supplies, as directed by the Elections Official.
- Verify that the required materials have been placed into the appropriate container(s), listing the materials inserted in each container and indicating that the container(s) were appropriately sealed.
- Return all transport media, paper ballots and supplies as directed by the elections official.

Returning Voted Ballots and Materials

Return all ballots and supplies as prescribed by the Election Code and as directed by the Election insert EC Official. (EC §14430-1435; 15550-15551; 17301-17306 (2005))

5.8 Securing audit logs and backup records

Procedures should be in place to insure that all audit logs are retrieved and retained and back up copies of all records should be retained as part of the official election. This includes the printing of the audit logs for the AccuVote-OS and AccuVote-TSX following the election and posting those audit logs at the respective polling places. Audit logs from the AccuVote-OS and AccuVote-TSX units should be retained and may be printed at the elections office as part of the semi-official canvass. The audit logs from the GEMS server should be printed and retained as part of the official records for the time period required by law.

5.9 Troubleshooting and problem resolution

Troubleshooting the AVPM

If the AVPM does not work properly due to paper jam, or the paper record is unreadable during the course of a voter verifying the paper audit trail, the poll worker will determine whether the voter has completed casting the voter's ballot. If the ballot has been cast, the poll worker will close the AccuVote-TSX for voting, until the issue is resolved. If the voter has not completed voting, the poll worker will cancel that existing electronic ballot and create a new voter card for the voter, sending the voter to another AccuVote-TSX unit to complete voting.

The poll worker will contact the county elections office for assistance and report the problem.

A new security canister and paper roll may be loaded into an AVPM, if it is determined that the printer is functioning, but the paper was jammed or the printer cover was not firmly locked in place to allow the print to be visible on the paper. If it is necessary to replace the security canister with a new one, the canister in the AccuVote-TSX at the time of the jam will be placed in the poll worker's election return supply bag or designated container and stored by the precinct captain / inspector until the close of polls. The canister will be returned with the election AccuVote-TSX units and supplies to the central location. The poll worker will make effort to insure the privacy of the voter's ballot.

If the AccuVote-TSX is the sole unit in the precinct and the voter is an ADA voter, a paper ballot could also be issued for assisted voting, if requested by the voter, if the AccuVote-TSX is closed.

If the AVPM is running low on paper, and the message indicating the paper is low is displayed, the poll worker will not allow voters to vote on that AccuVote-TSX until the paper roll and security canister is changed. The poll worker must use a new security canister and paper roll, take the old security canister and place it in the designated election return bag.

If the paper low message appears and it does not appear that the paper is low, the poll worker should verify the message by the opening the AVPM and if the paper is fine they will need to insert the Supervisor card to resume voting.

If the voter access card is ejected and the message appears that it was inserted upside down or incorrectly – the voter should notify the poll worker – the poll worker will reinsert the card in the AccuVote-TSX to verify and issue the voter a new card if necessary.

If a paper jam or the paper low message appears, and it appears that the paper has been misfed by a poll worker, the poll worker will contact the elections office for assistance. If the jam occurs during voting, the poll worker may be instructed to cancel the ballot and provide the voter with a new voter card. If the AccuVote-TSX is the sole unit in the precinct and the voter is an ADA voter, a paper ballot will be issued for assisted voting.

At no time will the security canister be opened to resolve a paper jam. It may be necessary to use a new security canister to resolve the paper jam. The poll worker will install the new security canister, take the old security canister and place it in the designated election return bag. At no time should the poll worker break the security seal on the security canister or open the old security canister.

If a paper jam occurs during the printing of the zero report, the security canister may be opened to resolve the paper jam, and then a new security seal would be put in place with the security seal number recorded. The security canister may not be opened if there are official election paper ballot audit trails in the security canister.

For AccuVote-OS Precincts

Some possible problems and their resolution are included below:

- NO Ballots - Inspector lost ballots/Car Crash, etc: A poll worker will have reported this problem to the office or hotline troubleshooting desk. The precinct inspector will be informed regarding whether to pick up ballots and where or whether they are to be delivered to the polling place.
- Can't Locate Ballot Box: The hotline troubleshooting desk will encourage the precinct inspector to continue looking for the ballot box. If they can't find it, the hotline troubleshooting desk could look in the jurisdiction warehouse to see who delivered and where they put the ballot box. If there is still no ballot box, the hotline troubleshooting desk will dispatch a ballot box to the precinct. The poll worker will be instructed to have the voters deposit voted ballots in "temporary ballot box" using AccuVote-OS bag, designated container or a ballot transfer bag.
- Forgetting to Bring AccuVote-OS: Until the problem is resolved, have the voters will deposit ballots in the side auxiliary bin of the ballot box. If this scenario happens, open the Left Side Auxiliary door (emergency slot) on the side of the ballot box with the keys that you have in the troubleshooter AccuVote-OS bag. Voting can proceed,

with voters depositing ballots in the side auxiliary bin, while the Inspector sends to obtain, or an AccuVote-OS arrives at the polling place.

- Lost AccuVote-OS / Car Crash, etc.: Until the problem is resolved, have the voters deposit the ballots in the left side auxiliary bin of the ballot box. Immediately call the hotline troubleshooting desk and let them know the polling place name needing the AccuVote-OS. Make arrangements to have AccuVote-OS with the memory card delivered in the most expedient manner (meet delivery person half way), or you may need to return to the Elections Office building to get an AccuVote-OS. When you get The AccuVote-OS at the precinct, it will already be in "election mode" and you will simply insert turn the AccuVote-OS on, following opening instructions. Explain to inspector that ballots in the side bin should be processed prior to running the ender card at the end of the day.
- Can't Close front door of Ballot Box: Occurs when the small arms in the top door are not lining up with holes on side of ballot box. Try having another poll worker help pull the AccuVote-OS back while trying to lock front door. If this doesn't work, they can operate AccuVote-OS with the front door down, until troubleshooter arrives.
- AccuVote-OS won't slide completely into ballot box: It is possible that the ballot box connector is not mating properly with the AccuVote-OS receptacle. This connection is used to run the ballot box diverter arm for sorting ballots. If the pins are bent on the ballot box, straighten them and try again. Sometimes the AccuVote-OS needs to be lifted very slightly while mating with the ballot box pins.
- Memory Card reads "OK to Format? " when AccuVote-OS is turned on: Until the problem is resolved, have the voters deposit ballots in the left side auxiliary bin of the ballot box. You can try pulling out the memory card and re-inserting it into the AccuVote-OS, and turn on AccuVote-OS again. Try this approach up to five (5) times. Sometimes the card is OK, but in traveling is loose and making bad connection. IF CARD STILL DOES NOT WORK, call the hotline troubleshooting desk and let them know the polling place name and that they will need to burn a new memory card for the precinct. Make arrangements to have memory card delivered in most expedient manner (meet delivery person half way), or you may need to return to the Elections Office building to get a memory card. When you get the new memory card at precinct, it will already be in "election mode," and you will simply insert it into the AccuVote-OS at the polling location. When you turn on the AccuVote-OS, it will print the zero totals tape. Follow the remainder of opening instructions.
- Memory Card reads "Generating Report" but is not printing zero tape: Check to ensure the print ribbon is properly set in the AccuVote-OS. If this doesn't correct the problem, have voters deposit ballots in the left side auxiliary bin of the ballot box. Call the hotline troubleshooting desk and let them know the polling place name.
- No Opening / Closing Instructions: The hotline troubleshooting desk can try and walk the inspector through the opening procedures over the phone or have the voters deposit ballots in the left side auxiliary bin until the troubleshooter arrives. When troubleshooter is on-site, give the inspector spare instructions from the troubleshooter bag, and help them open the polling place.
- "No Keys" in AccuVote-OS bag: The hotline troubleshooting desk will ask the poll worker to re-check the AccuVote-OS bag, including all pockets in the AccuVote-OS bag. If there is still no key, the hotline troubleshooting desk should instruct the poll workers to use a ballot transfer bag or an AccuVote-OS bag as a temporary ballot

box until the troubleshooter arrives. Have the voters continue voting, but deposit the ballots in a temporary bag or designated container.

- Key doesn't fit locks: The hotline troubleshooter desk can try and determine whether the inspector has two ballot box keys or two AccuVote-OS keys instead of one of each. If the inspectors have two (keys) that are the same, they can not open the polling place.
- If two ballot box keys: Have them open the Emergency / left side auxiliary bin and have the voters deposit the voted ballots here until the troubleshooter arrives. Until the problem is resolved, have voters deposit the ballots in the left side auxiliary bin of the ballot box. The troubleshooter will have to replace the keys when they arrive and then run the opening procedures per instructions. Instruct the inspector to run ballots from the emergency bin at end of day, prior to running the ender cards.
- Swapped black rubber key identifier: The hotline troubleshooting desk should also verify that perhaps the black key ring was placed on the wrong key, and they are simply trying the wrong key. If the inspector has one of each key type, it should work. If the inspector can't open poll, then the inspector will have to follow the "No keys" instructions above.
- If two AccuVote-OS keys: The inspector can't open polling place with ballot box. See "No Keys" above.
- 1st Ballot Won't go into AccuVote-OS: Verify that the ballot feed path is clear into the ballot box. The ballot slot may have the key positioned, so the lock arm won't allow the ballots to pass into ballot box. If so, insert the key into lock at ballot feed path and reposition lock arm.
- Printer jam: The troubleshooter should explain to the inspector to answer NO to need another copy during the opening instructions, and proceed with voting in a normal fashion. Replace and lock the AccuVote-OS printer cover until the troubleshooter arrives. The troubleshooter will reload the paper and ready it for the closing of the polls. The Audit trail on the memory card will show that the zero totals were run and the time they were run, so all voting will be accomplished normally without further problems.
- "Power Failure" flashing: The AccuVote-OS is not getting power and is running off the battery. It will operate approximately 2.0 hours without power. The hotline troubleshooting desk will first check the following:
 - Determine whether the AccuVote-OS is plugged into a wall outlet;
 - Determine if it is plugged into wall outlet that doesn't work (plug lamp or something into it to test outlet or just move it to another outlet);
 - Determine whether the power strip switch is turned to off setting;
 - Open the top door on ballot box, and gently slide the AccuVote-OS out far enough to see if power cord is still plugged into AccuVote-OS. If not, push it in firmly and relock

front door of ballot box, and continue voting;

- If the AccuVote-OS is still not working, dispatch a troubleshooter. The troubleshooter will figure out the location of the hot outlet, check all connections, or may need to replace the power cord. The troubleshooters will be given a spare power cord with the AccuVote-OS.
- "LOW Battery" Message: This message displays that the battery needs charging. Perhaps the on/off switch was turned on somehow during transporting the AccuVote-OS. The hotline troubleshooting desk can tell the p poll worker that the battery should charge up in a few minutes, assuming that there is power getting to the AccuVote-OS. Verify all connections are good. Tell the poll worker to open the emergency / left side auxiliary bin and deposit the voted ballots in the bin for approximately 10 minutes. Recheck the message display on the LCD. The message should be gone at this point and normal ballot processing can resume. Remind the poll workers to run the ballots in side bin prior to running the ender card. Tell the poll worker to call back if problem continues. If the problem continues, contact the hotline troubleshooting desk.
- Ballot Jams: The hotline troubleshooting desk will instruct the inspector to have the voters deposit the ballots in the left side auxiliary bin of the ballot box until the problem is resolved. The hotline troubleshooting desk will try and determine if problem is a "returned ballot" or a "counted ballot" (see error message section below).
 - *"Returned Ballot Jammed in Reader"*: If a ballot has jammed while it was trying to return it to the voter, the inspector should gently pull the ballot out of the AccuVote-OS (if they can access it from the front), or lower the front door of the ballot box, gently pull the AccuVote-OS out enough to see the jammed ballot from the rear of the AccuVote-OS, gently pull the ballot out, and relock the AccuVote-OS into ballot box. Resubmit the ballot.
 - *"Counted Ballot Jammed in Reader"*: If the ballot has jammed while it was trying to drop into the ballot box, the inspector should gently pull the ballot out of the AccuVote-OS (if they can access it from the front), or lower the front door of the ballot box, gently pull the AccuVote-OS out enough to see the jammed ballot from the rear of the AccuVote-OS, and gently pull the ballot out. The ballot should be manually inserted into the ballot box through the normal ballot slot path. Once completed, relock the AccuVote-OS into the ballot box. Unlock the bottom front lock on the ballot box and lift the ballot box lid. Look inside the ballot box (with any witnesses watching) and see if the ballots are caught on the diverter arm, or stack so that ballots can not fall into ballot box correctly. Fix any stuck or piled ballots.
 - *If jams are happening often*: The ballot box may have ballots piling up in the ballot path, preventing them from dropping in the ballot box bin. If this scenario happens, the troubleshooter, will unlock the bottom front lock on the ballot box, lift the lid, and determine how best to fix ballots that get caught in diverter arm or stuck.
- NO Ender Card: The ender cards have been placed in the AccuVote-OS bag in a pouch on the bottom half of the bag. This pouch is under the AccuVote-OS when they open up the bag. Poll workers may not notice this pouch. If the poll worker does not have an ender card, contact a troubleshooter in the field, or dispatch a

troubleshooter to the site. The troubleshooter(s) will have Ender Cards, and when he / she arrives, they can assist with the AccuVote-OS closing procedures.

- If it is late to obtain an ender card, instruct the poll worker to take the AccuVote-OS to the designated regional site drop off and explain to the regional personnel that they were unable to complete the closing procedures with the AccuVote-OS. The regional personnel can run an Ender Card and transmit results from the regional site.

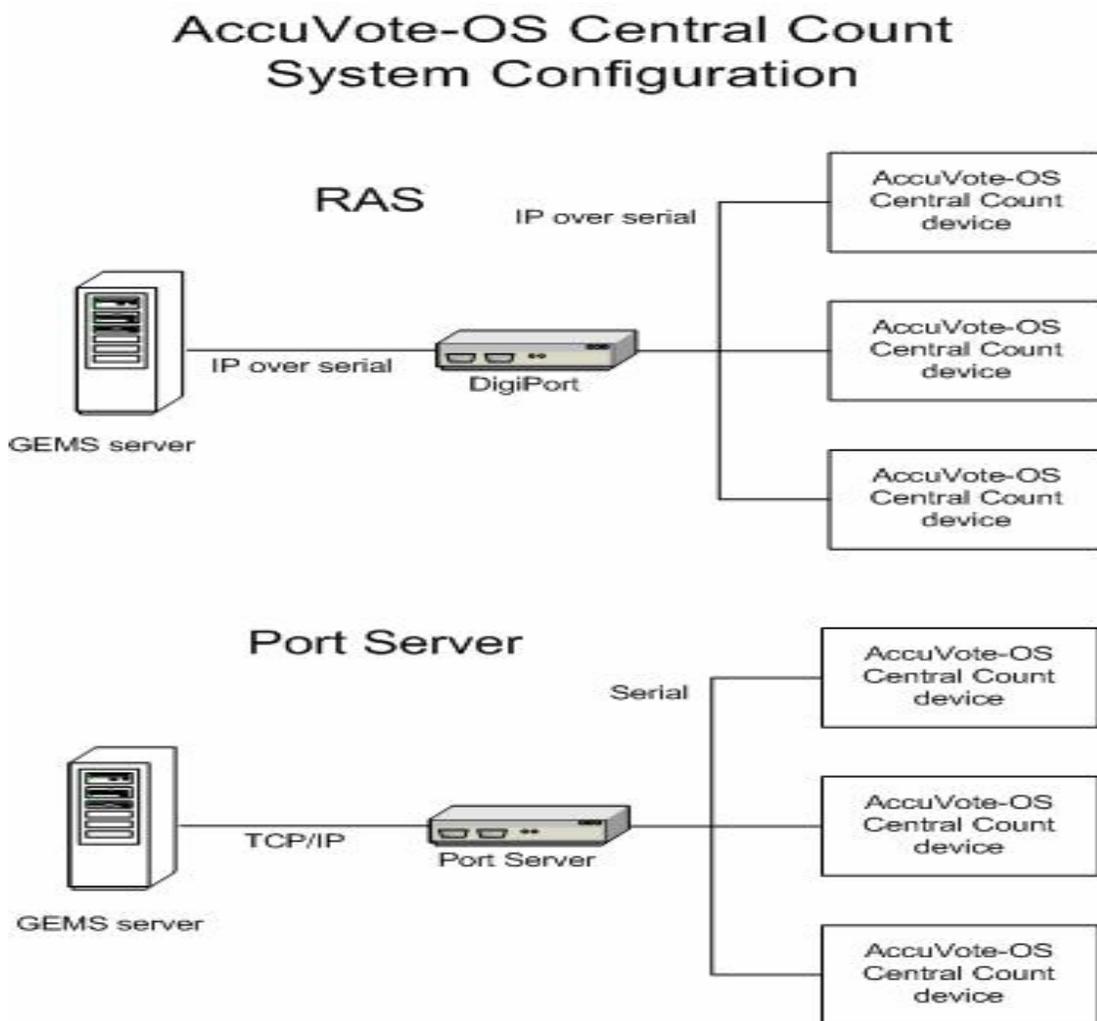
6 Absentee/Mail Ballot Procedures (central tabulation)

The AccuVote-OS Central Count is a batch ballot processing solution employing the AccuVote-OS ballot counting device configured with Central Count firmware, linked over a closed loop, local area network connection to the GEMS election management server.

The AccuVote-OS Central Count is useful for processing large volumes of mail ballots, such as absentee ballots. The AccuVote-OS Central Count mode allows any ballot type to be fed into the AccuVote-OS without any presorting of ballots. All that is required is that the vote center in which ballots are counted is logically associated with all election precincts to the vote center in the GEMS software.

The AccuVote-OS Central Count may be configured with multiple AccuVote-OS Central Count units linked to the GEMS server in either the local area network configuration or using Windows Remote Access Server (RAS). The AccuVote-OS Central Count may be scaled to accommodate the number of units, decks, and deck sizes required, while Ethernet-based local area network transmission between AccuVote-OS Central Count units and the GEMS server assures instantaneous results posting.

The picture below illustrates a sample Central Count setup:



GEMS is used to drive AccuVote-OS Central Count from the Central Count Server console, which provides an automatic and current live ballot count as ballot processing is in progress. All

Central Count administrative reporting functionality is offered in real time by GEMS, including deck counts by report precinct, by deck, and by posting time.

The AccuVote-OS Central Count employs all ballot validation logic of the AccuVote-OS, including the validation of control marks, such as the card ID, Diagnostic, and timing marks, card ID/precinct association, precinct/vote center association, white levels, and ballot stock weight. Ballots may be fed into the AccuVote-OS in any one of four orientations – face up, face down, head first, and foot first. Only valid AccuVote-OS ballots will be accepted by the AccuVote-OS, as generated by GEMS, and printed in conformance with Premier's *Ballot Specifications Guide*. Ballots processed in the AccuVote-OS Central Count may equally be processed in AccuVote-OS Central Count, AccuVote-OS Precinct Count.

Every valid ballot type may be tested on the AccuVote-OS Central Count unit using Unvoted, Fully Voted, and Count Tests. No test counts are introduced as a result of the Unvoted and Fully Voted Ballot Tests, and any counts resulting from processing test ballots may be easily reset in the GEMS database prior to Election Day. Please refer to AccuVote-OS Central Count Users Guide for more detail on these tests.

In addition to these ballot tests available in Central Count mode, the AccuVote-OS Central Count firmware also supports the setup and diagnostics modes. The setup mode is used to configure the AccuVote-OS Central Count device for central counting, while Diagnostics Mode is used to perform diagnostics tests on the AccuVote-OS device, including verifying its ability to log on to the network, display information on the LCD, test system memory, the AccuVote-OS printer, the main serial port, the auxiliary serial port, and the card reader. Setup and diagnostic modes are detailed in the AccuVote-OS Central Count Users Guide.

6.1 System startup and pre-tabulation report procedures

The detailed start up, running and tabulation procedures may be found in the Central Count Users Guide.

6.2 Tabulation procedures

Central Count is driven from the GEMS Central Count Server console. This console is divided into three tabs: Machines, Decks and Log.

The Machines tab displays all machines that are currently actively counting ballots in Central Count mode, and includes the deck number, the Central Count AccuVote-OS IP number, the machine status, and the current ballot count in the deck. Only machines are displayed that are actively counting ballots.

The Decks tab displays the numbers of all ballot decks that have been counted, the completion time, and the total deck count.

The Log records all batch start and end transactions, as well as any batch processing error conditions that have arisen. Those log reports can be printed from GEMS.

Disabling the Central Count Server console does not clear any of the decks counted and recorded under the Decks tab. Centrally counted ballot decks may be deleted either by selecting the decks under the Decks tab, and clicking on the Delete button, or by resetting election results. Once the Central Count Server console has been readied, the Start button is disabled, and the Stop button is enabled.

Note that the Central Count Server console is modeless, that is, it may be accessed at the same time as the GEMS main window. The election status cannot be changed as long as

the console is active. As ballots are being centrally counted, monitor AccuVote-OS Central Count units to verify that equipment idle time is minimized. Review the Log occasionally, ensuring that any error messages that may arise have been properly accounted for.

Any decks that have been counted in previous central count sessions are listed under the Decks tab only once central count has been activated for the vote center under the Machines tab.

Careful reconciliation logs should be maintained daily to account for all ballots processed.

6.3 Post tabulation report and shutdown procedures

The central count reconciliation should occur immediately after shutdown to assure the jurisdiction that the correct number of ballots has been tabulated.

The central count reports from GEMS in the Administrative reports screen should be used to reconcile deck numbers with actual ballots processed and any discrepancies investigated.

These include:

- Central Count Status Report by Deck
- Central Count Status Report by Time
- Central Count Status Report by Race
- Central Count Status Report by Report Precinct

7 Semi-Official Canvass Tabulation and Reporting

7.1 System start-up and pre-tabulation reports

The Election Official responsible for the conduct of an election shall assign staff or appoint boards to carry out the following semi-final official canvass functions:

- a. Absentee Voter and Provisional Voter Ballot Processing
- b. Seal and Container Inspection
- c. Ballot Processing
- d. Ballot Duplication
- e. Memory Card control
- f. Elections Observer Panel
- g. Other boards deemed necessary by the responsible Election Official. Individuals appointed may perform more than one function, or serve on more than one board
- h. Print the following reports from GEMS prior to shutting down and backing up for the evening:
 - Election Summary Report
 - AccuVote-TSX status report
 - AccuVote-OS status report
 - Cards Cast report
 - AccuVote-TSX write-in reports

The semi-final official canvass functions listed above must be performed by a minimum of two persons. Each board member shall be appointed to perform the function designated.

All applicable reports should be assembled and be available – procedures should be in place to reconcile precinct returns, absentee returns, and provisional ballots. Provisional ballots and any absentees from the polls should be prepared for resolution and presentation to the Canvass Board.

The Election Official shall establish procedures to account for all voted ballots, results tapes, security canisters, memory cards during the semi-final official canvass.

The Write-in ballots should be validated to those valid write-in candidates.

Absent Voter and Provisional Voter Ballot Processing:

Absent voter ballots and provisional voter ballots, returned to polling places on Election Day, are sealed in designated containers by precinct boards for return to the designated counting location. These designated containers shall be removed from the precinct supply kits on election night or the next day if properly secured. The condition of the seals shall be noted and reported as required by the Election Official.

Absent voter and provisional voter ballots received on election night shall be:

- a. Processed on election night in accordance with these Procedures and the Elections Code; or
- b. Maintained in a secure location accessible only to the Election Official under controlled conditions before being processed.

Ballot Duplication

Correcting or duplicating defective ballots shall be done in a clear, unambiguous, and auditable manner such that the voter's mark and intent is preserved and the Election Official's action adheres to the voter's intent. For defective absentee or mail ballots and / or ballots where the voter intent is clear, but the AccuVote-OS cannot read the ballot, the ballot shall be processed according to the following procedures (defective ballots may be duplicated before processing or after rejection by the AccuVote-OS units, or both).

1. When an absentee or mail ballot voter takes corrective action on their ballot and voter intent is clear, the Election Official may use a Post-it Correction & Cover-up tape in lieu of duplicating a complete ballot to cover extraneous marks made by the voter or to allow the Election Official to enhance a mark made by the voter. The Election Official may make a designated unique mark on the tape so long as the tape could be removed and the original mark made by the voter is preserved. The Election Official shall initial next to this correction in an area in which it will not be interpreted as a vote.
2. When an absentee or mail ballot is insufficiently marked and the voter's intent is clear, e.g., ballot ovals filled in with red ink, light pencil or other light marks, then the ballots are to be duplicated or corrected following either or both of these procedures:
 - a) The Election Official may use a Post-it Correction & Cover-up tape lieu of duplicating a complete ballot to cover marks made by the voter or to allow the Election Official to enhance a mark made by the voter. The Election Official may make a designated unique mark on the tape so long as the tape could be removed and the original mark made by the voter is preserved. This unique mark or enhancement shall take the form of a slash mark on the tape covering the original oval the voter has indicated. The Election Official may make the mark so that it is sufficiently different in color and style and cannot be mistaken as the voter's original mark. The Election Official shall stamp or initial to this mark in an area on the ballot where the mark was enhanced by the elections official or authorized designee in which it shall not be interpreted as a vote.
 - b) The Election Official may use a colored translucent marker (such as a highlighter) that will not obscure, obliterate, or otherwise destroy the voter's original mark but will create a mark that is readable by the AccuVote-OS. The Election Official shall initial next to this mark in an area in which it shall not be interpreted as a vote.
 - c) When an absentee or mail ballot timing marks are defective, corrective active may be taken by duplicating the ballot and processing the ballot; or (2) repairing the timing mark.

Duplicating defective ballots.

Deliver defective voted ballots to the appropriate location for processing. All ballots prepared as duplicates of defective voted ballots shall be of a distinctive color, or be identifiable by other distinguishing means, clearly labeled "duplicate," and shall be given a serial number which shall also be recorded on the damaged ballot.

In creating the duplicate ballot, one board member shall duplicate voting positions marked on the original/damaged ballot, and shall enter a facsimile of the write-in vote(s), if any. Efforts need not, and should not, be made to match the handwriting characteristics of the voter when entering these write-in facsimiles. Particular attention must be paid to completing or not completing the ovals opposite the write-in spaces as the voter has done, or failed to do. Another member shall verify that the voting position marks and write-in entries (including oval completions or lack thereof) on the duplicate ballot match those in the damaged ballot.

Duplicates shall be placed with voted ballots of the appropriate precinct for further processing, tallying, and storage. The original ballot, which has been duplicated, shall be distinctively voided, placed in clearly identified containers for duplicated ballots, and segregated in a secure location so they cannot be counted inadvertently.

7.2 Processing vote reports

7.2.1 Central tabulation

All central count reconciliation logs and central count logs used for an election should be assembled and compared for accuracy. Errors and deficiencies should be investigated and resolved.

7.2.2 Precinct tabulation

Poll book signatures and ballots cast reports should be compared for any discrepancy. Results tapes and results reports should be compared for accuracy. Errors and deficiencies should be investigated and resolved.

7.2.3 Integration with county systems and the Calvoter system

Unofficial results should be transmitted and verified with the reports from GEMS and the results tapes returned from the polls. Appropriate information should be transmitted to the appropriate systems *e.g., voter history, unofficial vote totals to the CalVoter system.

The California Secretary of State template files should be linked to export results to the Cal Voter system. Optionally, vote totals may be manually entered directly into the CalVoter system by a designated official.

8 Official Canvass and Post-Election Procedures

In order to assure the privacy of the voters, the County should establish procedures that assure the separation of duties between those who canvass the returns and those who work the polls.

The Official Canvass consists of a post-election audit of the voting 'precincts' returns and the absent voter ballot returns. The canvass is designed to:

- Validate the outcome of the election by verifying that there were not more ballots cast than the sum of the numbers of voters who signed the precinct Roster / Index, and who applied for and were issued absent voter ballots;
- Account for all official ballots produced for the election; to ensure that all required certificates and oaths were properly executed by the precinct board;
- Verify the accuracy of the computer count by manually recounting the voted ballots from at least one percent of the voting precincts and comparing the manually-tallied results to the computer-generated results;
- Process any provisional ballots;
- Process any valid write-in votes;
- Resolve any ballot exceptions;
- Certify the Election results.

8.1 Election Observer Panel

All procedures prescribed in this manual shall be carried out in full view of the public insofar as feasible. In addition, the responsible elections official shall devise a plan, subject to the approval of the Voting Systems Panel, whereby all critical procedures of the vote tallying process described in this Manual are open to observation by an Election Observer Panel. Representatives of the qualified political parties and representatives of the news media shall be among those invited to serve on this Panel and shall be given the opportunity to observe that the correct procedures have been followed in the receiving, processing, and tallying of all the voted ballots. The Election Official shall appoint an Election Observer Panel; failure of any or all invited parties to participate on the Panel shall not stop procedures from continuing as otherwise required by law.

8.2 Canvassing precinct returns

The processing of precinct ballots returned from the precinct during the canvass shall not be done by poll workers but by those appointed by the County Elections Official.

The recommended procedures for processing precinct ballots returned from the precinct during the canvass are as follows. This includes the return of precinct provisional ballots from the precincts.

- Verify eligibility of persons who cast ballots provisionally according to the Guidelines for Processing Provisional / "Fail-Safe" Ballots in an Election, as provided by the Secretary of State;

- Open envelopes of eligible voters and remove ballots;
- Examine ballots for write-in votes, noting cause for rejection and damage;
- Identify original or duplicate provisional ballots by precinct and deliver to the designated official for updating computer tallies;
- Write the reason for rejection on envelopes of ineligible voters. Place unopened envelopes with election materials to be retained for the period prescribed by law;
- Examine the Ballot Statement prepared by each precinct board;
- Compare the number of official ballots reported “received” by each precinct to the number issued by the elections official. Resolve or explain any discrepancy;
- Verify that the number of ballots voted (including those voted provisionally), plus spoiled and unused ballot cards, equals the number received by the precinct. Resolve or explain any discrepancy.

Reconcile tallies

- Compare the number of signatures in the Roster-Index to the number of precinct voter ballots reported on the Ballot Statement. Resolve or explain any difference between the two;
- Compare the number of ballots voted by provisional and precinct voters to the Summary reports and/or results tapes. Resolve or explain any discrepancy;
- Locate any ballots not counted on election night because of damage, invalid identification marks, improper orientation, or any other reason;
- Search election supplies and equipment, including unused and spoiled ballots, write-in envelopes, ballot containers, etc., for ballots not accounted for.

8.3 Canvassing Absentee returns

The elections official is accountable for absentee ballots to the same extent, as nearly as practicable, as for precinct ballots. The duties include:

- Prepare a Ballot Statement for each ballot type or special absent voter “precinct” showing the number of ballots produced (received), any defective ballots received from the vendor, spoiled or damaged ballots, the number of returned ballots that were challenged, and the number to be counted;
- Reconcile the statement to demonstrate that the total of unused, defective, spoiled, issued, and replaced ballots equals the number received. Resolve or explain any discrepancy;
- Compare the computer count to the number of ballots to be counted, as shown on the Ballot Statement. Resolve or explain any discrepancy.

8.4 Canvassing provisional ballots

The processing of absentee and precinct provisional ballots returned from the precinct during the canvass shall not be done by poll workers but by those appointed by the County Elections Official. The recommended procedures are as follows:

- Verify eligibility of persons who cast ballots provisionally according to the Guidelines for Processing Provisional/"Fail-Safe" Ballots in an Election, as provided by the Secretary of State;
- All AccuVote-TSX provisional ballots that require further investigation should be printed from GEMS and attached to the appropriate envelope to be processed according to established State Law and County procedure. All valid AccuVote-TSX provisional ballots shall be accepted in GEMS and the tallies updated;
- For AccuVote-OS provisional ballots, open envelopes of eligible voters and remove ballots;
 - Verify eligibility of persons who cast ballots provisionally according to the Guidelines for Processing Provisional / "Fail-Safe" Ballots in an Election, as provided by the Secretary of State;
 - Open envelopes of eligible voters and remove ballots;
 - Examine ballots for write-in votes, noting cause for rejection and damage;
 - Identify original or duplicate provisional ballots by precinct and deliver to the designated official for updating computer tallies whether those are paper provisionals;
 - Write the reason for rejection on envelopes of ineligible voters. Place unopened envelopes with election materials to be retained for the period prescribed by law.

8.5 Canvassing write-in votes

All ballots containing write-in votes must be examined by the Write-In Processing Board or a board established by the county elections official and / or designee. The recommended procedures are as follows:

AVOS Manual Recount Procedures

The recommended procedures for the AVOS manual recount procedures for write-in votes are to examine the voting positions on the ballot for the office where the write-in vote occurs. The AccuVote-OS tabulator will have scanned each ballot and determined the oval markings for that ballot. If the write-in vote created an overvote condition, the ballot would have returned to the voter/operator for action. If the voter has marked the name on the regular ballot and written in the name on the ballot on the write-in line, the election official shall ensure that the vote is tabulated one time only. If the name is written in only and is not marked on the candidate list, the election official may determine the voter's intent to select the candidate.

- a. To be considered as a write-in vote, the oval next to the write-in space must be marked and /or filled-in (EC 15342).
- b. If the name written in is not on the Certified List of Write-in Candidates, the write-in vote shall not be counted.
- c. If the write-in vote is for a qualified candidate in the precinct and does not constitute an overvote, the write-in vote is manually tallied.

AccuVote-TSX Manual Recount Procedures

GEMS will indicate the number of votes cast for each write-in position for each contest. GEMS has the AccuVote-TSX write-in reports that will also contain the actual write-in candidate's name cast by the voter as recorded on the AccuVote-TSX units. Immediately after results are uploaded for AccuVote-TSX units, the GEMS database shall be backed up with the established naming convention. This will also be done prior to closing down the server at the end of the evening.

Prior to any reconciliation of qualified write-ins, the jurisdiction may (1) print the AccuVote-TSX ballot images from GEMS; (2) print the applicable write-in summary reports; or (3) tally the write-in totals from the AVPM.

The local officials will tally and record the write-in votes cast for write-in candidates from this report. In tallying the write-in votes in a contest designated as a "Vote for Two" or more, the election official may encounter a name written in that is the name of a ballot qualified candidate. In this instance, the election official shall check the ballot image report to determine whether the ballot qualified name written in is also marked on the list of candidates.

8.6 Manual recount procedures

For the purpose of validating the accuracy of the computer count, a public manual tally of the ballots cast should be conducted as to all candidates and ballot measures voted on in each of the precincts.

For the manual tally, the AVPM paper audit trail and ballots shall be tabulated by hand using county established procedures.

The recommended procedures for counting on the AVPM are as follows:

- Print out the applicable precinct summary report in GEMS
- Print out the ballot images from the vote center that were uploaded compare the actual AVPM record to the ballot images from GEMS to further validate the results
- Manually tally the results from the AVPM and compare the tally to the precinct reports from GEMS. If the VVPAT summary and the Gems Summary are different, it must be determined if a manual counting mistake has occurred. If an error has occurred, the error must be reconciled.
- The County should take measures to assure an accurate manual count is conducted of the VVPAT summary reports and no person who worked at that polling location should be allowed to conduct this count.

8.7 Handling ballot exceptions

The precinct and/or absentee ballots may contain writing or marks that could identify the voter. These ballots must be examined by the Elections Official. If the marks WOULD IDENTIFY the voter, the ballot should be rejected and placed it in the designated container. Names, addresses, and initials are considered identifying marks.

If the marks WOULD NOT IDENTIFY the voter, process the ballot along with all other valid ballots. The following specific standards shall be used in determining if one or more marks on an AccuVote-OS ballot are to be included in the count.

Marked Voting Position Oval

A vote shall be considered valid and included in the count when the marked voting position oval is completely filled in.

Other Marked Ballots

A vote shall be considered valid and included in the count when the voter has marked the ballot in a clear and understandable manner such that a pattern or patterns are discernable.

Table B also lists instances when a voted ballot may or may not be counted.

TABLE B

<i>SHALL BE COUNTED</i>	<i>SHALL NOT BE COUNTED</i>
B.1. When the voter, instead of completely filling in the voting position oval, clearly and consistently indicates voting choices by placing a mark, such as an "X" or a "√" or circling the candidate's name or voting position oval or uses a combination of marks such that a pattern or patterns identify the voter's intent, the votes shall be counted.	B.8. If a voter places marks on a ballot which identify the voter, the ballot shall not be counted. Initials by a mark correcting a vote do not by themselves identify the voter.
B.2. When the voter, instead of completely filling in the voting position oval on the official ballot, clearly and consistently indicates voting choices by placing a mark, such as an "X" or a "√" or circling the candidate's name or voting position oval or uses a combination of marks such that a pattern or patterns identify the voter's intent on the sample ballot rather than on an official ballot, and mails the sample ballot in the absentee envelope, the ballot shall be duplicated and counted.	B.9. If a voter transmits his or her voted ballot by facsimile, without an original signature, the ballot shall not be counted.
B.3. When the voter indicates voting choices by writing the name(s) of the candidate(s) or indicating the vote(s) on a proposition(s) in a letter or note, and returns it in an absentee envelope, the ballot shall be duplicated and counted.	
B.4. If the voter writes correcting instructions anywhere on the ballot card, or on a note accompanying the card, and the note does not identify the voter, the ballot shall be counted.	
B.5. If the voter marks a vote selection, but attempts to erase or otherwise correct this voting choice, and clearly makes another voting choice, this vote shall be counted.	
B.6. If a voter uses the write-in portion of the ballot to indicate a voting choice for a candidate or measure that is listed on the ballot, the vote shall be counted.	

SHALL BE COUNTED	SHALL NOT BE COUNTED
B.7. If the voter uses the write-in portion of the ballot to indicate a voting choice for a candidate listed on the ballot, and also marks the designated voting position oval for the same candidate, the ballot shall be counted as one vote for that candidate.	

8.8 Post election logic and accuracy testing

A Post-Election Logic and Accuracy Test similar to the Pre-Election Logic and Accuracy Test may be performed following the election at the County's discretion.

Post-Election Logic and Accuracy Testing is addressed in the GEMS Election Administrator's Guide.

8.9 Final reporting of official canvass

The official canvass consists of a post-election audit of the polling place returns and the absent voters returns and serves to;

- Validate the outcome of the election by verifying that there were not more ballots cast than the sum of the numbers of voters who signed the precinct Roster/Index and who applied for and were issued absent voter ballots;
- Ensure that all required certificates and oaths were properly executed by the precinct board;
- Verify the accuracy of the computer count by manually recounting the voter ballots from the authorized recount requirements that include comparing the manually-tallied results to the computer-generated results and the paper audit trails.

The Final results shall be verified and delivered to the Secretary of State in the manner prescribed by law.

8.10 Backup and Retention of election material

Upon the certification of the election results, Elections Code sections 17300 through 17506 apply to the handling, security and disposition of unused ballot cards and other elections materials. The retention period for ballots and related election materials is six months for all elections if no federal elections are involved. The federal election retention period is twenty-two months. The retention periods may be extended in the event of a court challenge.

All ballot tabulation operations including mandated pre-and post-election testing, must be documented in sequential order. An automated and/or manual record or log must be maintained to record the time and date of "system events" related to ballot counting. All associated election materials must be retained for the period prescribed by law. Copies of the election database should be date and time stamped and preserved as well. They may be in the form of cd or other media.

System events in the ballot tabulation process include:

- Initiation of the ballot count program

- Clearing totals
- Running logic and accuracy tests
- Hardware Failures
- Repairing hardware (including running accuracy tests after repairs are completed)
- System crashes and restarts
- Communications between multiple systems
- Lost communication to remote sites
- Time communication is restarted

The GEMS Audit log shall be continued until final certification of results, shall be printed and retained for this same time period as ballots for that election, and shall be subject to the same physical security and integrity measures.

Specific audit trails may include:

- Exception Handling/Error Messages During Ballot Tabulation, such as;
- AC offline
- System status messages, such as:
- Polling Place Open and Close

9 Manual Recount procedures

A request for a recount and the conduct of the recount shall be made in accordance with Elections Code section 15600 with the following:

Public Observation

The recount shall be conducted publicly.

Appointment of Spokesperson

Upon request, the elections official shall determine the candidates and or campaigns or others that are parties of interest in the recount, and each party of interest shall appoint a spokesperson who shall act as a contact person between the election official and the party of interest. The spokesperson shall be authorized by the party of interest to make final decisions on behalf of the candidate or campaign. The spokesperson shall have access to all parts of the recount area when accompanied by an Election Official. The spokesperson may appoint other persons to observe the recount process, the number and activities of such persons depending on procedures established by the Elections Official.

Order of Precincts

The person requesting the recount may specify the order of precincts to be counted, and may specify whether the recount begins with precinct ballots, absentee ballots, provisional ballots, or other types of ballots. In the absence of such a request, the elections official shall determine the order in which precincts are counted. Any change to the order must be requested in writing by the candidate or campaign, or the designated spokesperson.

Ballot Security

The elections official shall provide for the security of ballots during the recount process. The costs for any security measures in addition to those determined necessary by the elections official that are requested by the voter requesting the recount and that are approved by the elections official shall be added to the cost of the recount.

Cost of Recount, Daily Deposit

The voter filing the request seeking the recount shall, before the recount is commenced, deposit with the elections official a sum as required by the elections official to cover the cost of the first day of the recount. For subsequent days, no later than 3:00 pm the day before each day's recount, the requestor shall pay to the elections official a sum sufficient for the next day's recount, as determined by the Election Official. If the advance deposits are not paid, the Election Official will terminate the recount.

Examination of Ballots and Other Materials

Any research, review, or handling of relevant election material, as defined in Elections Code section 15630, shall be done at the discretion of the Election Official. Requests to research, review, or handle relevant materials must be in writing and must be received by the elections official before the recounting of ballots is complete. The requestor shall pay all additional costs to complete the research or review. One or more representatives of each party of interest, as determined by the elections official, may be present for any research or review of relevant materials conducted under this section.

Interference with the Recount Process

No person appointed as an observer may interfere with the recount process. All questions must be directed through the designated spokesperson directly to the elections official or his or her designee. No questions or remarks of any kind may be directed to any member of the recount board. No observer may touch or handle ballots.

Procedure to Challenge Ballots

Ballots may be challenged according to the provisions of Elections Code section 15631. The elections official shall, prior to the recount, establish a procedure for review and resolution of challenges. This procedure shall include, but is not limited to, notice to all interested parties of the rules, regulations, and procedures that will be used to resolve challenges.

10 Security

10.1 Physical security of system and components

Introduction

Physical security is paramount to running accurate and secure elections. Each jurisdiction should address the need to maintain and achieve this goal. As part of preparing for an election, each jurisdiction should review its physical security processes and procedures, and identify best practices for maintaining and improving those processes and procedures. This section defines some of the steps for each jurisdiction in establishing and maintaining procedures for physical security. The main goal for the elections official in maintaining these processes and procedures for physical security is ensuring the protection of the election tally process from intentional manipulation, fraudulent manipulation, fraudulent and intentional manipulation, malicious mischief, accidents, and errors. As part of ensuring physical security of the election system and components, each jurisdiction should:

- a. Procedures: System Changes — These procedures may also include a check list and sign-off requirement for the system proofing tasks.
- b. Procedures: Physical Protection — Establish procedures for the physical protection of facilities, and data and communications access controls as appropriate for the facility and equipment. The procedures shall also include provisions for locked facilities for computers as well as for voted and non-voted ballots and counted and uncounted ballots.
- c. Procedures: Technical Security – Establish procedures for the technical security of the system, including the establishment and maintenance of passwords, system and database backup, administrative privileges and access to those privileges, among others.
- d. Procedures: Internal Security — Establish procedures for internal security, i.e., the protection of ballot counting hardware, firmware, and software from fraudulent manipulation by persons within the elections office. These procedures should address:
 1. Restricted access to ballot counting hardware, firmware, and software;
 2. Develop processes for ensuring no malicious attack or tampering has occurred on the election equipment;
 3. Processes for a standalone election network protected from malicious attack or tampering;
 4. Individual passwords which must be complex and frequently changed;
 5. Physical protection of all non-voted precinct and absent voter ballots, as well as of all tallied and non-tallied ballots to chronicle their use and access before and after the election.
- e. Contingency Plan — Establish contingency plans for ballot counting, including either backup ballot counting facilities under the elections official's supervision, or a reciprocal agreement with a neighboring jurisdiction to count ballots in the event of hardware failure. This should include the develop of a risk assessment plan to identify risks and disaster recovery plans in the event of a hardware failure. In addition to the ballot counting program sent to the Secretary of State, each elections official should store another copy of the ballot counting program in a secure-but-readily-accessible location.

A copy of each County elections official's security procedures should be on file in the office of the election official.

In addition to the above procedures, the jurisdiction should establish procedures to identify and certify individuals who may observe the ballot counting and tabulation process, pursuant to California election law. All unescorted persons present within the security area, including visitors, media representatives, and standby personnel, shall be clearly identified by a badge or other means and a log of their arrival and departure times. All unescorted personnel shall be subject to restrictions established by the responsible elections official to ensure the efficiency, transparency and integrity of the vote tallying process.

Election Security Plan

Each jurisdiction should develop an Election Security Plan that addresses the following areas of security. The areas of security include the ballot tabulation program, the precinct counting system, and other peripheral systems and components. The following areas are recommendations based on prior recommendations for improving security of the ballot tabulation system, and best practices for security of the ballot tabulation program.

Security of the Ballot Tabulation Program (GEMS server)

1. Election Officials shall maintain the GEMS Server is in a controlled, preferably locked area with access limited to authorized staff and personnel.
2. Access to the GEMS server shall be tightly controlled and all persons having access to the server at any time, shall be pre-approved by the county elections official and noted in a log that details the name, date and time of access to the room in which the GEMS is housed.
3. Election Officials shall verify that no Direct Access Oriented (DAO) capable program has been installed or resides on GEMS server. DAO programs include but are not limited to MS EXCEL, MS ACCESS, and other Visual Basic programs designed to work with Direct Access Objects.
4. The GEMS server shall be set to require user login. Administrative user logins should be limited to only those times user accounts need to be set or changed or software needs to be installed or updated. For routine use, a lesser user account should be used. An administrative user should also be issued an additional, separate user account for routine use if their duties require routine election use.
5. A minimum of two people in the county election office shall have administrative access to the server supporting GEMS (the ability to set or change passwords). Additional user accounts may be assigned at less than administrative access but all users shall have and use separate user account with unique usernames and passwords. The administrative users' passwords shall meet or exceed Microsoft Windows password guidelines for a strong password. Lesser user accounts should be at least as strong as the GEMS passwords. The second administrative user username / password should be stored in a sealed envelope placed in a safe as part of a disaster recovery plan but should not be used for routine use.
6. Network connections, including the GEMS network, should be local.

7. The GEMS server computer and communications systems shall be used for election purposes only.
8. Election staff shall not install third-party software on the GEMS server system that has not been previously approved for use by Premier.
9. Whenever software and / or files are received from any external entity, this material must be tested for unauthorized software on a standalone, non-production machine before it is used on the GEMS server system. If a virus, worm, or Trojan horse is present, the damage will be restricted to the involved machine.
10. Approved virus checking programs must be continuously enabled on computers supporting the GEMS server system. Premier recommends McAfee virus scan. The virus checking programs should be updated and a virus scan ran immediately prior to any election.
11. Externally supplied floppy disks, CDs or DVD's may not be used on any GEMS server unless these disks have first been checked for viruses and deemed to be free of such viruses.
12. If unofficial summary results from the GEMS server are to be distributed or published, the information should be exported from GEMS to a file on the server and then copied to electronic media (e.g., floppy disk, CD). That electronic media can be taken to a separate computer system that has external connections to the Internet for export.
13. Back-ups of GEMS databases should be performed using electronic media (e.g., CD). Users must ensure that the back-up is labeled with the time and date of the back-up and signed by the person who authorized and performed the back-up. Additionally, the GEMS election database should be backed up periodically.
14. No voting terminal or other component of the voting system will have wireless technology installed or have any ability to allow the transmission of vote results through wireless technology.
15. The boot option shall be set to hard drive only with the BIOS secured by a password. The password shall follow industry standards for a secure password.

Security of the Precinct Counting Systems

Security of AccuVote-TSX units

The following are areas for improving security of the AccuVote-TSX unit, and best practices for security of the AccuVote-TSX unit:

1. All AccuVote-TSX units shall be upgraded to use software that requires SSL/TLS standards and be documented.

2. New encryption keys using the Key Card Tool (KCT) shall be created and used for Administrative and Supervisor Smart Cards and AccuVote-TSX units for each election. These keys will be stored in a secure location with limited access by county election staff until needed for use.
3. Security keys shall be verified and logged as they are changed.
4. No PIN shall use only the digits "0" and "1".
5. Each memory card shall have a permanent serial number assigned to it.
6. The county shall maintain a chain-of-custody log that accurately records the chain-of-custody of each memory card and AccuVote-TSX unit from the point of programming the memory card for use in the election through the time of completion of the official canvass.

The chain of custody log can be created for the county to record and track the serial number of each security seal placed on the AccuVote-TSX unit. The chain-of-custody log would be used to verify the correct security seals are on the AccuVote-TSX, and have not been tampered. An example of a chain-of custody log is below:

TSX Chain of Custody Form

District#: _____ **Precinct#:** _____ **Precinct Name:** _____

County: _____ **Election:** _____

		OUT			IN			
TSX Serial Number	Privacy Panel Seal Number	Election Data Compartment (Upper) Seal Number	Election Data Transport Compartment (Lower) Seal Number	Transporter Initials (After Delivery)	Privacy Panel Seal Number	Election Data Compartment (Upper) Seal Number	Election Data Transport Compartment (Lower) Seal Number	Transporter Initials (After Return)
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
Designated Warehouse Personnel's Signature:					Designated Warehouse Personnel's Signature:			
Transporters' Name Printed:					Transporters' Name Printed:			
Date Picked Up:					Date Picked Up:			
Signature of Transporters:					Signature of Transporters:			

7. All AccuVote-TSX units shall be sealed across the halves of the unit with a serialized tamper-evident seal such that the unit cannot be open or disassembled without breaking the seal. A log shall be maintained of such seals assigned to each AccuVote-TSX unit. The integrity of that seal shall be verified after programming each AccuVote-TSX unit for an election, prior to opening the polls, immediately upon closing the polls, and upon return of the AccuVote-TSX unit to the jurisdiction's headquarters after the election. The authorized poll worker shall verify and validate the security seals have not been tampered prior to, and upon closing of the polls. The county may also choose to seal other areas of the AccuVote-TSX with tamper-evident seals for additional security. The chain-of-custody log shall be signed by the authorized poll worker.
8. If a violation of the tamper evident seal is discovered prior to the start of the election, the elections official or designated person will investigate and determine the appropriate course of action. If an elections official or designated person has determined a violation has occurred, the AccuVote-TSX unit shall be immediately taken out of service and the violation inspected by the chief election official or designated person and reported to the Secretary of State. If a violation of the tamper evident seal is discovered after the start of the election, the chief election official or designated person will investigate and determine if a security violation has occurred. If a security violation has occurred, and the election official or designated person has determined a security violation has occurred, the unit shall be taken out of service and all votes cast on the AccuVote-TSX unit will be manually tabulated.
9. Prior to inserting the memory card into the AccuVote-TSX unit to complete the programming of the unit for an election, the Ballot Station firmware will be reinstalled from a trusted version. That trusted version is may be provided by the California Secretary of State's office. This process is accomplished by placing a memory card with a trusted version of the software into the AccuVote-TSX while it is powered off and turning the unit on. To complete the instructions, follow the procedures provided by Premier and the AccuVote-TSX on-screen instructions.
10. If prior to an election, there is a legitimate question about the secure chain of custody with respect to an install memory card or the Ballot Station firmware on an install memory card, the chief elections official or designated person will investigate and determine an appropriate course of action if a violation has occurred with respect to the secure chain of custody on the install memory card or the Ballot Station firmware on the install memory card. If the chief elections official or designated person has determined that a violation has occurred with respect to the secure chain-of-custody on the install memory card or the Ballot Station firmware on the install memory card, all AccuVote-TSX units programmed with the install card will be immediately taken out of service and any votes all ready cast on an AccuVote-TSX will be manually tabulated and reported from the AVPM paper audit trail. The Secretary of State will be notified of this event.
11. Each memory card shall be programmed in a secured facility under the supervision of the registrar of voters or registrar of voters' staff. The memory card(s) shall be inserted into the assigned AccuVote-TSX unit as soon as

practicable and a serialized, tamper-evident seal shall be immediately applied to the AccuVote-TSX memory card door. The county may also choose to seal other areas of the AccuVote-TSX with tamper-evident seals for additional security. Once a memory card is programmed for the election, the chain-of-custody log shall be immediately updated upon insertion of the AccuVote-TSX memory card(s). The chain-of-custody log shall be updated upon insertion of the memory card and have the AccuVote-TSX units' serial number and the memory card serial number logged into the chain-of-custody tracking sheet designed for that purpose.

12. The county shall maintain a chain-of-custody log that records which memory cards and which serialized tamper-evident seals is assigned to which AccuVote-TSX units. Any breach of control or break in the chain-of-custody log determined to have occurred prior to Election Day of the memory card and or AccuVote-TSX unit or tamper-proof seal shall require that a replacement memory card should be programmed and issued in the presence of two election officials or designated persons.
13. On Election Day, prior to any ballots being cast on any unit, the integrity of the tamper-evident seal(s) shall be verified by the precinct officer before opening the AccuVote-TSX. The serial number of the seal shall also be verified against the log provided to the precinct officer. This procedure shall be witnessed by at least one other precinct officer or staff of the registrar of voters.
14. If there is a discrepancy between the tamper evident seal log and the serial number(s), the discrepancy shall be confirmed by one or more of the remaining members of the precinct board, documented, and immediately reported to the county elections official for the jurisdiction. The elections official or designated official will investigate and determine the appropriate course of action. If a discrepancy is determined to have occurred, The AccuVote-TSX shall be taken out of service until the election official determines the appropriate course of action.
15. If being used to meet the accessibility provisions of federal or state law, or if for any reason only one such unit is being used at the precinct, the county will establish poll worker training procedures to mitigate one vote being cast on the AccuVote-TSX unit. The procedures should establish methods that can be used by poll workers to attempt to have at least two more ballots are cast on the machine, even if not by a voter needing its accessibility components, in order to protect the privacy of the voter.
16. The County will be responsible for procedures for maintaining a chain-of-custody log throughout the Election Day process, including return of the memory card to the election office or drop-off location. Security transport bags will be used during the transport phase of the memory card back to the drop off location or election office.
17. If, upon return of the sealed memory card in the AccuVote-TSX or sealed memory card transport bag, it is determined that a potential breach of the seal has occurred, the breach must be investigated by the appropriate elections

officials and appropriate steps should be taken as a result of those findings in the investigation. Reconciliation should also establish whether any discrepancies for total votes between the memory card and the AccuVote-TSX.

Security of AccuVote-OS units

The following are areas based on prior recommendations for improving security of the AccuVote-OS unit, and best practices for security of the AccuVote-OS unit:

1. Each memory card shall have a permanent serial number assigned to it.
2. The county shall maintain a written chain-of-custody log that accurately records the chain-of-custody of each memory card and AccuVote-OS unit from the point of programming the memory card for use in the election through the time of completion of the official canvass.
3. Each memory card shall be programmed in a secured facility under the supervision of the registrar of voters or registrar of voters' staff. The memory card(s) shall be inserted into the assigned AccuVote-OS unit as soon as practicable and a serialized, tamper-evident seal shall be immediately applied to the AccuVote-OS memory card security bar. The county may also choose to seal other areas of the AccuVote-OS with tamper-evident seals for additional security. Once a memory card is programmed for the election, the chain-of-custody log shall be immediately updated upon insertion of the AccuVote-OS memory card(s). The chain-of custody log shall be updated upon insertion of the memory card and have the AccuVote-OS unit serial number and the memory card serial number logged into the chain-of-custody tracking sheet designed for that purpose.
4. The county shall maintain a chain-of-custody log that records which memory cards and which serialized tamper-evident seals is assigned to which AccuVote-OS units. Any breach of control or break in the chain-of-custody log prior to Election Day of the memory card and/or AccuVote-OS unit or tamper-proof seal shall require that the memory card shall be replaced in the presence of two election officials.
5. On Election Day, prior to any ballots being cast on any unit, the integrity of the tamper-evident seal(s) shall be verified by the precinct officer. The serial number of the seal shall also be verified against the log provided to the precinct officer. This procedure shall be witnessed by at least one other precinct officer or staff of the registrar of voters.
6. If it is detected that the tamper-evident seal has been broken prior to turning on the AccuVote-OS , or if there is a discrepancy between the log and the serial number, the discrepancy shall be confirmed by one or more of the remaining members of the precinct board, documented, and immediately reported to the county elections official for the jurisdiction. The unit shall be taken out of service until the election official investigates and determines the appropriate course of action.
7. The County will be responsible for procedures for maintaining a chain-of-custody log throughout the Election Day process, including return of the memory card to the election office or drop-off location. Security tamper evident seals will be used during the transport phase of the memory card back to the drop off location or election office.

8. If, upon return of the sealed memory card in the AccuVote-OS or sealed memory card transport bag, it is determined that a potential breach of the seal has occurred, the breach must be investigated by the appropriate elections officials and appropriate steps should be taken as a result of those findings in the investigation. Reconciliation should also establish whether any discrepancies between the memory card and the AccuVote-OS, as well as the summary reports occurred.
9. Any replacement seals shall be logged and verified using a log designed for that purpose,

10.2 Logical security of system and components

This section lists the system service components that should be implemented for the voting tabulation system. This includes services and ports, passwords, anti-virus protection, and other components. The procedures can be found in the Windows Configuration Guide and the Client Security Policy. There may be other requirements as needed:

10.2.1 Essential and non-essential services and ports

- All network services and network ports are to be turned off, except those explicitly required to run the GEMS software;
- the “auto run” feature in Windows is to be disabled;
- the boot order is to boot from the hard drive only;
- the BIOS is to be password protected to prevent changes to the boot order;
- The specifics for understanding and implementing these items can be obtained from Premier.

10.2.2 User-level security

GEMS Passwords

A minimum of two people in the county election office shall have usernames and passwords with administrative access to the GEMS election database (These may be different than the server administrators and are specific to the election). The GEMS passwords shall be at least 6 to 8 digits and include a combination of alpha and numeric characters.

Passwords shall be changed before each election. Each user should immediately change the password, if the password is suspected of being disclosed, or is known to have been disclosed, to an unauthorized party.

Users are responsible for all activities performed with their personal login-IDs. Login-IDs may not be utilized by anyone but the individuals to whom the log-ons have been issued. Users shall not allow others to perform any activity with their login-IDs.

The GEMS server, workstation, or terminal should not be left unattended without first logging-out or invoking a password-protected screen saver, as is practicable with security procedures and best practices for administering elections.

10.2.3 Anti-Virus protection

An anti-virus program shall be installed. Premier recommends MacAfee virus scan. The virus program shall be updated and a virus scan run immediately prior to each election. The current and updated dat files should be downloaded on another system, virus checked and then installed and verified.

10.2.4 Procedures for verifying, checking, and installing essential updates and changes

Software to be loaded to the server should be virus scanned and also verified to come from an authorized source. The software may be provided by the California Secretary of State's Office. Once verified, the software should be installed and retested to verify the software is correctly functioning.

10.2.4.1 Audit records for the changes showing what, when, who, and why

A log of the server should be kept to track what is on the server and what is installed by whom and when. This should be done by a minimum of 2 people and the log signed by each individual.

10.2.4.2 Installation procedures

Updates should be received via CD through the mail or downloaded on a secure system and then virus scanned and transferred to the GEMS server once validated.

Software to be loaded to the server should be virus scanned and also verified to come from an authorized source. The software may be provided by the California Secretary of State's Office. Once verified, the software should be installed and retested to verify the software is correctly functioning.

10.2.4.3 Acceptance testing after the installation.

Verify that all of the expected functionality of the GEMS workstation is available. Mark each function on a signoff sheet, once it has been verified. The following functions are to be verified:

1. Copy from CD
2. Restore database
3. GEMS version
4. Reports version
5. View card in Card Editor
6. Print ballot artwork
7. Print administrative reports
8. Record/play back audio
9. Download memory card
10. Upload memory card

11. Print results report
12. Perform a backup
13. View GEMS User's Guide
14. Verify GEMS "Read Me" file
15. JResult Client version

10.3 Security procedures for central processing

The following are some best practices for ensuring the security of the central ballot processing system:

- a. Ballots processed at the central location shall be secured from tampering, theft and damage in the same way that official ballots are secured.
- b. Appropriate physical, technical and administrative processes and procedures shall be in place to ensure security of the central processing system.
- c. Voting units utilized for early voting shall be secured at the end of each day and appropriate security logs shall be kept.
- d. Election material used on a daily basis (e.g., voter access cards, VCProgrammer, AccuVote-OS and AccuVote-TSX units, Supervisor and Administrator cards and, official ballots) shall also be secured when not in use.
- e. The server shall be secured and locked when not in use and only used by authorized personnel. This includes the voting equipment connected to the server.

Security of Votes

Tampering, Theft, Alteration — The elections official shall ensure the security of all votes cast are free from tampering, theft, or alteration, and shall ensure that the results of votes counted exactly reflects the number of voters and the voter's selections.

Voting on Multiple Days — If early voting takes place on more than one day, the elections official shall establish procedures to reconcile each day's voting activity and to ensure that votes and other activities have been recorded and securely stored. The number of votes cast each day shall be compared to the number of voters who appeared requesting to vote and who were authorized to vote, as determined by the roster, or by other means.

Voted Ballots Returned to Elections Office — Voted ballots from each day's voting shall be returned to the elections office, and an audit trail produced and preserved documenting the results from each day's voting.

Storage at Election Warehouse

If the memory cards is to be installed in the voting terminals prior to distribution to the vote centers, the voting terminals should be kept in a secure location after the memory card installation. The location should restrict access to only authorized personnel. Logs shall be kept to track the memory card installation.

Secure Storage — Voting devices shall be securely stored when not in use. Storage should be in a locked location, with access to that location authorized by an election official or designee.

10.4 Security procedures for polling place

The following are some best practices for ensuring the security of the precinct ballot processing system:

Storage at Vote Center

After distribution of the AccuVote-OS and AccuVote-TSX units to the vote centers, the units should be kept in a secure location at the vote centers. The location should restrict access to only authorized personnel. If possible, appropriate to protecting the security of the voting location, tamper-evident seals and other security mechanisms should be placed on entries into the secure location.

The AccuVote-OS and AccuVote-TSX units shall be inventoried, sealed and verified. Any discrepancies should be noted and rectified prior to opening and setup on Election Day. The discrepancies should be immediately reported to the authorized election official or designee.

Election supplies, such as, rosters, official ballots, signs, shall be kept in the possession of the designated election official and verified and inventoried according to established procedures.

10.5 Audit trails

All system audit logs for software and hardware should be retained as part of the official elections record. The Logic and Accuracy test results as well as maintenance and repair logs should also be maintained. This should include the audit logs for the precinct equipment used for an election.

See the following sections for procedures related to the audit logs.

Section 12.6 of the GEMS User Guide details printing the audit logs for the GEMS software.

Section 4.10 of the Ballot Station User Guide details printing the audit logs from the AccuVote-TSX.

Section 13 of the AccuVote-OS Precinct Count User guide details printing the audit logs from the AccuVote-OS.

List of Reference / User Manuals

The following is a list of reference / user manuals related to the Premier AccuVote® system:

1. AccuFeed_1.0_Hardware_Guide
2. AccuView_Printer®_Module_Hardware_Guide
3. AccuVote®-OS_Central_Count_2.00_Users_Guide
4. AccuVote®-TSX_Hardware_Guide
5. AccuVote®-TSX_Pollworkers_Guide
6. AVPM_Service_Guide_Revision
7. AVPM_Single_Roll_Opening_and_Closing_Procedures
8. GEMS®_1.18_Election_Administrators_Guide
9. GEMS®_1.18_Product_Overview_Guide
10. GEMS®_1.18_Reference_Guide
11. GEMS®_1.18_System_Administrators_Guide
12. GEMS®_1.18_Users_Guide
13. Key_Card_Tool_4.6_Users_Guide
14. VCProgrammer_4.6_Users_Guide
15. Voter_Card_Encoder_Users_Guide
16. Ballot_Station_4.6_Users_Guide
17. AccuVote®-OS_Precinct_Count_1.96_Users_Guide
18. AccuVote®-OS_Pollworkers_Guide

State of California

AUDIT USE PROCEDURES

Premier Election Solutions, Inc.

These procedures are proposed for adoption by the California Secretary of State pursuant to the Conditions of Re-approval of Premier Election Solutions AccuVote®-OS and AccuVote®-TSX.

These procedures shall be effective only upon approval by the Secretary of State and shall be used in conjunction with all other statutory and regulatory requirements. Insofar as feasible, all procedures prescribed herein shall be carried out in full view of the public.

These procedures constitute a minimum standard of performance. They are not intended to preclude additional steps being taken by individual election officials to enhance the integrity and reliability of the auditing process.

Submitted

October 2, 2007

State of California Audit Use Procedures

Introduction

Premier Election Solutions, Inc. (Premier) has been working with California counties to provide those counties with election equipment, supplies and services since 1993. Since that time, Premier has been working with the counties on providing best practices in the areas of election administration, management, as well as election processes and procedures.

This *Audit Use Procedures* document describes the approach recommended by Premier in carrying out vote results auditing and accounting, review of audit logs and retention of election documentation to validate vote results, and detecting of unauthorized manipulation of vote results; however, Premier believes it is outside the scope of the voting system vendor's responsibilities to be involved in the auditing procedures utilized by a local jurisdiction. This document is based on best practices from several California counties in providing election services and support. This document is intended as a guideline for counties in auditing processes and procedures with Premier voting systems used in the State of California. **It is recommended that each jurisdiction consult with their State Election Authority in respect to applicable laws, regulations, procedures and other guidelines, which may impact how this information is used.**

This document is presented as part of the California Secretary of State's Conditions for Re-approval item number 18. Additional information is also found for auditing and use procedures in the Premier California Use Procedures document, submitted to the California Secretary of State on September 17, 2007.

Vote Results Auditing and Accounting

Each jurisdiction is responsible for carrying out the vote results auditing and accounting functions following each election. The period, referred to as the canvass, is a period in which the county reconciles the precinct roster signatures (number of signatures) to the number of voted ballots to the tapes on the AccuVote-OS (AVOS) and / or AccuVote-TSX (AVTSX) to the Election Summary Report in GEMS for that specific precinct. The Statement of Votes Cast (SOVC) report can also be used for verifying the total number of voted ballots match the number of signatures on the precinct roster.

The following are examples of the steps used for verifying this process. These steps are examples based on best practices adopted by several jurisdictions in California.

Step 1: Compare the number of voted ballots on the AVOS or AVTSX with the number of ballots counted on the Election Summary Report or the SOVC report.

1. Write the date and names of the canvass members on the top of each worksheet used for comparing the total number of voted ballots on the AVOS or AVTSX with the number of ballots counted on the Election Summary Report or SOVC report.
2. Begin with the first precinct and write the precinct number in the space provided on the worksheet.
3. Write the total number of ballots counted from the Election Summary Report or the SOVC report for the precinct in the space provided on the worksheet.
4. Write the total number of AVOS or AVTSX ballots counted in the precinct from the AVOS or AVTSX results tape for the precinct. If there are multiple precincts on the election summary tape(s), be sure to record the number of voted ballots from the correct precinct onto the worksheet.
5. Subtract the number on the results tape from the number on the Election Summary Report or the SOVC report. The result should be zero.
6. If the numbers balance, no further action is needed, unless verification is required.
7. If the result is not zero, recheck the numbers and if necessary, recount the ballots.
8. If a discrepancy remains, then further investigation is required.

Step 2: Compare the number of ballots issued to the precinct Inspector before Election Day with the total number of ballots in the precinct when the polls close.

1. Write the date and names of the canvass members on the top of each worksheet used for comparing the number of ballots issued to the precinct before Election Day with the total number of ballots in the precinct when the polls close.
2. Begin with the first precinct and write the precinct number in the space provided on the worksheet.
3. Add the total number of ballots cast, spoiled and unused in the precinct.
4. Subtract this total from the total number of ballots issued to the precinct. The result should be zero.
5. If the numbers balance, no further action is needed, unless verification is required.
6. If the result is not zero, recount each category of ballot.
7. If a discrepancy remains, then further investigation is required.

Step 3: Compare the number of cast ballots with the number of voters who signed the Roster.

1. Write the date and names of the canvass members on the top of each worksheet used for comparing the total number of cast ballots with the number of voters who signed the precinct roster.
2. Begin with the first precinct and write the precinct number in the space provided on the worksheet.
3. Add the total number of cast ballots, regular and provisional, in the precinct.
4. Subtract this total from the total number of voters who signed on the white, yellow and supplemental pages of the Roster. The result should be zero.
5. If the numbers balance, no further action is needed, unless verification is required.
6. If the result is not zero, perform the following:
 - Recheck your calculations. For example, check the addition of the different categories of ballots.
 - Recount signatures in the Roster. Staple the tape with your final count to the front cover of the Roster.
7. If a discrepancy remains, then further investigation is required.

In the event of any malfunctions during Election Day, as a result of power failures or other issues which could cause a possible disruption in the voting process, there are mechanisms to recover any possible loss of data. These mechanisms are documented in the following Premier user documentation:

BallotStation 4.6 User's Guide, Rev. 3.0.

- Section 4.4.2, Printing ballots
- Section 8.6.5, Restoring election results
- Section 8.6.6, Restoring election results to a new memory card

AVPM Auditing Mechanisms

During the canvass, the paper audit trail from the AccuView Printer Module (AVPM) is used to compare the total number of ballots cast in the AVTSX to the total number of ballots recorded on the AVPM. In the event of a discrepancy or recount, the AVPM is

the official record. Section 8 of the *Premier California Use Procedures* further describes the steps necessary to conduct a manual count on the AVPM.

During the canvass process, the paper audit trail from the AVPM is utilized to conduct a manual tally of the votes cast on the AVTSX. Part of this process includes detecting any abnormal patterns on the AVPM, which includes the identification of paper jams or the identification of cancelled or rejected ballots. Part of the canvass process will be to identify any abnormalities on the AVPM for the specified precinct for which the manual recount is occurring.

There are several Premier product documents which provide further information on addressing and resolving abnormalities with the AVPM. Those documents include:

AccuVote-TSX Pollworker's Guide, Rev.5.0

- Section 12.2, Troubleshooting, Election Day

AccuView Printer Module Service Guide Rev. 1.1

- Section 2.8, Metal platen backward rotation
- Section 2.9, Metal platen forward rotation
- Section 2.10, Paper advancement
- Section 2.11, Take-up spindle canister rotation
- Section 2.16, Paper visibility in viewing window
- Section 2.17, No information printed
- Section 2.18, Incorrect information printed
- Section 2.19, Hourglass display does not clear
- Section 2.20, Paper take-up
- Section 2.22, Printing vibration

Additionally, the county, in the event of a discrepancy between the AVPM and the total number of votes cast, should perform the following (note: discrepancies could occur as a result of a paper jam on the AVPM, or incorrect threading of the paper roll into the AVPM):

1. Compare the total number of votes cast on the AVPM paper audit trail to the total number of votes cast from the Election Summary Report or the SOVC for the specified precinct.
2. If the numbers balance, no further action is needed, unless verification is required.
3. If a discrepancy exists, print out the cast ballot images from the AVTSX or from GEMS for the specified precinct; and

4. Count the total number of ballots cast from the AVPM and the cast ballot images and compare the results.
5. If the numbers balance, no further action is needed, unless verification is required.
6. If a discrepancy remains, then further investigation is required.

Audit Trails

GEMS Audit Trails

The Global Election Management System (GEMS) has several audit mechanisms to verify and detect the modification of vote results in GEMS. The main GEMS audit log lists the steps performed by the User/Administrator of the GEMS system. Each entry describes the steps taken by the User/Administrator within GEMS. This log includes, but is not limited to creating the election, generating ballots, setting the system for election, downloading and uploading the memory cards, reporting, and conducting recounts.

This main GEMS audit trail also provides for detection of modification of vote results by stating which precinct, which user and which contest was modified. It lists every instance of that event.

There are other audit logs in the GEMS application. The AV Results Server shows:

- the number of memory cards for both the AccuVote-OS and / or the AccuVote-TSX downloaded or uploaded,
- the date and time for those occurrences, and
- the connections for downloading and uploading those memory cards.

The Central Count Server log shows:

- the connection of the central count units to GEMS, and
- the decks committed or deleted from GEMS.

Additionally, to prevent unauthorized access to GEMS, the GEMS server is configured to allow for access to the system via a password into the operating system, as well as to GEMS.

AccuVote-OS and AccuVote-TSX Audit Trails

Both the AVOS and the AVTSX have the ability to audit and print out audit log reports. The audit logs in GEMS can be viewed and printed, but no audit log entries can be deleted in GEMS. The information on viewing and printing GEMS audit log information can be found in Section 12.6 of the *GEMS User Guide* and Section 3.46 of the *GEMS Election Administrators Guide*.

The audit log reports includes, but is not limited to:

- System and election information
- Date and time the unit:
 - was set for election,
 - was turned on or off,
 - had the counters cleared,
 - had the election ended,
 - had reports printed,
 - entered supervisor functions.

For the AVTSX, the audit functionality includes the key steps for system function as well as the audit features for the specified election on the election media. Additionally, the AVTSX audit lists when the election was downloaded and uploaded.

Appendix A – Archiving and Restoring AccuVote-TS Logs Using Soft Media

A.1 Introduction

This Appendix describes the process by which AccuVote-TS audit log and election results information stored on a memory card are stored on soft media such as a computer hard disc or CD-ROM and subsequently retrieved. In short, after an election, security key information and the contents of the AccuVote-TS memory cards are stored onto the soft media of choice (hard disc, CD-ROM) and securely stored. When the audit or election information stored on the soft media is later needed, the contents of the media are read back onto blank memory cards, one or more AccuVote-TS units are security keyed to match the keys used in the election under study, the units are loaded with the memory cards containing the needed information and that information is available on the subject AccuVote-TS units.

A.2 AccuVote-TS Audit Logging

All system operations performed on the AccuVote-TS unit are logged to the unit's System Log. All election related operations are logged to the Audit Log. When an installed memory card has been programmed with election data, system operations are logged to both the Audit Log and the System Log. The Audit Log is stored on the memory card and the unit, and the System Log is stored on the unit only.

The System log is accessed using the View System Log function on the Ballot Station-Main Menu (Pre-Download Mode) screen. The Audit Log may be accessed from Pre-Election Mode, Election Mode or Post-Election Mode screens. Either log is printed using instructions found elsewhere in these Use Procedures or in *BallotStation User's Guide*, sections 3.1.3 and 4.10.

A.3 Note Regarding Memory Cards

Election and ballot information displayed on the AccuVote-TS unit is determined by the data downloaded to the installed PCMCIA memory card. For additional security, election/ballot information and results of voted ballots are automatically saved on both the memory card and the AccuVote-TS unit's internal hard disk drive.

The election mode (Pre-Election, Election or Post-Election) that the AccuVote-TS unit is set to is also saved on the installed memory card. This allows the card to be used on any AccuVote-TS unit encoded with the same security keys. When the card is inserted into a new unit, election, ballot, and any results data is automatically copied to the unit's internal hard disk drive, and the unit's System and Audit logs are updated (including the Audit log on the memory card). The new unit displays the election on the memory card exactly as it was displayed on the previous unit.

A.4 Security Keys

IMPORTANT: Once audit information is stored onto soft media, it cannot be restored and re-used unless the security keys used in that particular AccuVote-TS unit were also saved and are available for use when the audit log information is retrieved. Jurisdictions MUST ensure that security key information is securely stored along with the audit log information in a usable, organized, and retrievable format so that persons restoring audit information in the future are able to retrieve the keys to install into one or more AccuVote-TS units. Failure to properly maintain security keys will render the stored audit information irretrievable.

AccuVote-TS units running Ballot Station 4.6 support the use of user defined security keys and passwords. Security keys are a series of values that may be encoded on all Premier branded smart card reading devices. When properly defined on the election equipment, the security keys are copied to every voter access card created with or inserted in the card readers of these devices. Smart cards encoded with security keys that do not match the keys on the encoded device cannot be read; moreover, repeated attempts to authenticate these cards may cause them to be permanently disabled. Election results data recorded on encoded AccuVote-TS units is also encoded with security keys. Results data encoded with security keys may only be viewed on AccuVote-TS units encoded with the same security keys.

Security keys are implemented on all of the smart card reading devices using a Key Card, a smart card created using the Key Card Tool application. Users may view a popup screen with information on Ballot Station security status by touching the small key icon in the bottom right corner of the display.



Election results data recorded on encoded AccuVote-TS units is also encoded with security keys. Results data may only be viewed on AccuVote-TS units encoded with the same security keys. User defined security keys are created using the Key Card Tool. This PC- based application is used in conjunction with an external smart card reader device, allowing users to create a smart card encoded with user-defined security keys. This 'Key Card' is then used to copy the security keys to every AccuVote-TS, Voter Card Encoder, VCProgrammer and Election Media Processor unit that will be used in the election. The Key Card Tool is also used to encode Supervisor and Central Administrator type smart cards with the election's security keys, and to update the card's PIN. If user defined security keys are used, all cards used in the election must also be encoded with these keys. Security keys implemented on the election's voting equipment are changed from election to election.

Note: Although user defined security keys may be used when running Ballot Station 4.6, all cards used on AccuVote-TS units installed with this version must be encoded with a PIN. For more information on creating and using Key Cards, see the *Key Card Tool User's Guide*.

A.4.1 Implementing security keys on AccuVote-TS units

Use the following steps to define security keys on all AccuVote-TS units to be used in the election with the Key Card you have created.

Note: It is essential that election equipment security keys be encoded in a controlled environment by authorized staff only. It is also essential that user-defined security keys be implemented in a systematic and complete manner; that security keys are documented and that the affected equipment is carefully labeled.

AccuVote-TS units are encoded with security keys before the PCMCIA memory cards are programmed. If security keys are changed while a memory card that containing election data is installed on the unit you will not be able to load the current election after exiting the security settings screen. You will also be unable to restore election files from Archive without resetting the security keys on the unit to the keys used when the archive file was created.

To implement security keys on the AccuVote-TS Unit:

1. Power on the AccuVote-TS unit with no PCMCIA card installed.
2. Insert a Central Administrator card into the card reader. Enter the password and touch the OK button. Remove the card from the reader.
3. Touch the System Setup button.
4. Touch 'Security Settings' in the functions list to display the Security Settings options.
5. Touch the Update Keys button. The message "Please insert a security key into the card reader, or press the Cancel button." is displayed.
6. Insert the Key Card defined with the election's security keys into the card reader. The message "Ballot Station security settings have been updated. Please remove the security key

card.” is displayed.

7. Touch the Save Settings button and then touch the Close button. Touch the Exit Administration button.
8. Place a sticker on each AccuVote-TS unit encoded with security keys. The sticker should identify the version of the Key Card used to encode the unit as well as the Key Signatures displayed on the System Configuration>Security Settings screen when the keys have been updated. **This step is critical if different Key Cards will be used to encode the units with different security keys for different elections.**

A.4.2 Verifying security key implementation on AccuVote-TS units

Use the following procedure to verify that each of the Key Card's security keys have been correctly updated on all AccuVote-TS units and all cards to be used with these units:

1. Power on the AccuVote-TS unit with no PCMCIA card installed.
 2. Identify a card containing the updated Smart Card Key, Data Key and PIN.
 3. Insert the card into the updated AccuVote-TS unit.
 4. If the updated AccuVote-TS unit accepts the updated card, the AccuVote-TS and card are synchronized and using the new Smart Card Key.
 5. If the Smart Card Key on the card does not match the Smart Card Key encoded on the AccuVote-TS unit, the card will be rejected. If the card is accepted on the unit but the PIN number that is entered by the user does not match the PIN number encoded on the card, the card will be rejected.
 6. Set the AccuVote-TS for election and cast ballots.
 7. Remove the PCMCIA card from the AccuVote-TS.
 8. Identify a second AccuVote-TS unit which has not been updated with the same Data Key.
 9. Insert the PCMCIA Card into the second AccuVote-TS unit.
- The election will be displayed on the touch screen, but the number of ballots cast will appear to be zero. This is because the second AccuVote-TS unit cannot read the results on a PCMCIA memory card which has been encoded with a different Data Key value.

Note: The number of ballots cast on the memory card will be correctly displayed when the card is inserted into an AccuVote-TS unit encoded with the correct Data Key value.

This procedure demonstrates that the Data Key value is different on the two AccuVote-TS units, and confirms the key change on the updated unit.

A.5 Post-election Procedure

After the election and canvass, obtain a computer with a card reading device attached to it. This computer needs to comply with the Use Conditions as it will be in contact with election media, in other words, it needs to be known to be free of unapproved and malicious software. Read each memory card's contents into this computer using standard Windows or Mac copy commands. It is best to create a file for each AccuVote-TS unit, with a filename corresponding to that unit's serial number and/or precinct assignment. Once again, be sure to save the security keys associated to each AccuVote-TS unit in an organized fashion along with the memory card contents. Write the collected memory card contents to CD-ROM using commercial-off-the-shelf software. Be sure to read back at least a few memory card contents from the CD-ROM to ensure that it is properly written and suitable for use as archive media.

A.6 Preparing to Retrieve Audit/Election Information: Changing/Re-loading security keys on AccuVote-TS units

Use the following steps to change security keys previously defined on an AccuVote-TS unit. Unless a unit has the same keys used during the election for which audit information is being retrieved, this procedure must be executed so that the keys on the subject AccuVote-TS match those from the past AccuVote-TS unit for which audit information is being retrieved.

IMPORTANT: It is essential that election equipment security keys be encoded in a controlled environment by authorized staff only. It is also essential that user-defined security keys be implemented in a systematic and complete manner; that security keys are documented and that the affected equipment is carefully labeled.

When you are changing the security keys on an AccuVote-TS unit to restore audit information and/or election results that were archived using different security keys, you must create both a Key Card and Supervisor card with the security key values used to encode the election you wish to restore. See your election administrator for the

documentation of the archived election's security keys. For instructions on creating a Key Card, see the *Key Card Tool User's Guide*.

1. Power on the AccuVote-TS unit with no PCMCIA card installed.
2. Insert a Supervisor card encoded with the current security keys into the card reader. Enter the PIN and touch the OK button. Remove the card from the reader.
3. Touch the System Setup button.
4. Touch "Security Settings" in the functions list to display the Security Settings options.
5. Touch the Update Keys button. The message "Please insert a security key into the card reader, or press the Cancel button." is displayed.
6. Insert the Key Card defined with the election's security keys into the card reader. The message "Ballot Station security settings have been updated. Please remove the security key card." is displayed.
7. Touch the Save Settings button and then touch the Close button. Touch the Exit Administration button.

Note: When the security keys have been updated on the unit, you must use a Central Administrator card encoded with the updated security keys to access the updated unit's Administration functions. Ensure that updated Supervisor and Central Administration cards are created with the Key Card defined with the election's security keys.

A.7 Accessing the Election/Audit Information

1. From the archive media (CD-ROM or other as chosen), place the contents of the desired memory card from the election under study onto a clean memory card by copying its contents through Windows or Mac commands.
2. Place the freshly filled memory card into an AccuVote-TS unit that has been keyed to have the same security keys as the corresponding AccuVote-TS used in the actual election under study.
3. Use AccuVote-TS screen commands found elsewhere in these Procedures to view and/or print the audit and election information desired.

A.8 Optional Procedure for printing audit log information

Auditing the Memory Card in Pre-Election Mode only causes the Audit report to be printed. Auditing the Memory Card in Post-Election Mode prints the Audit report in addition to setting the Election Status Indicator to 6 (the election status is printed on the Audit report).

1 Press YES in response to:

- Print Audit Report?;
- then you will see
- Generating Report...;
 - Printing Label;
 - Printing Audit Report; and
 - Need another Printout?

To print another copy of the Audit report, press YES, otherwise press NO.

A.9 Viewing Audit Logs on the AccuVote-TS display

In Election Mode, pollworkers can access the Pollworker Options menu by inserting a Supervisor card and a correct password. This menu allows pollworkers to perform their election day duties, such as creating Voter Access cards, viewing the Audit Log, resuming voting, or shutting down the machine. This menu is also used to end the voting when the election is over. County officials can choose to make this function available to pollworkers or to leave it unavailable. If made available, the County is responsible for training regarding its use.

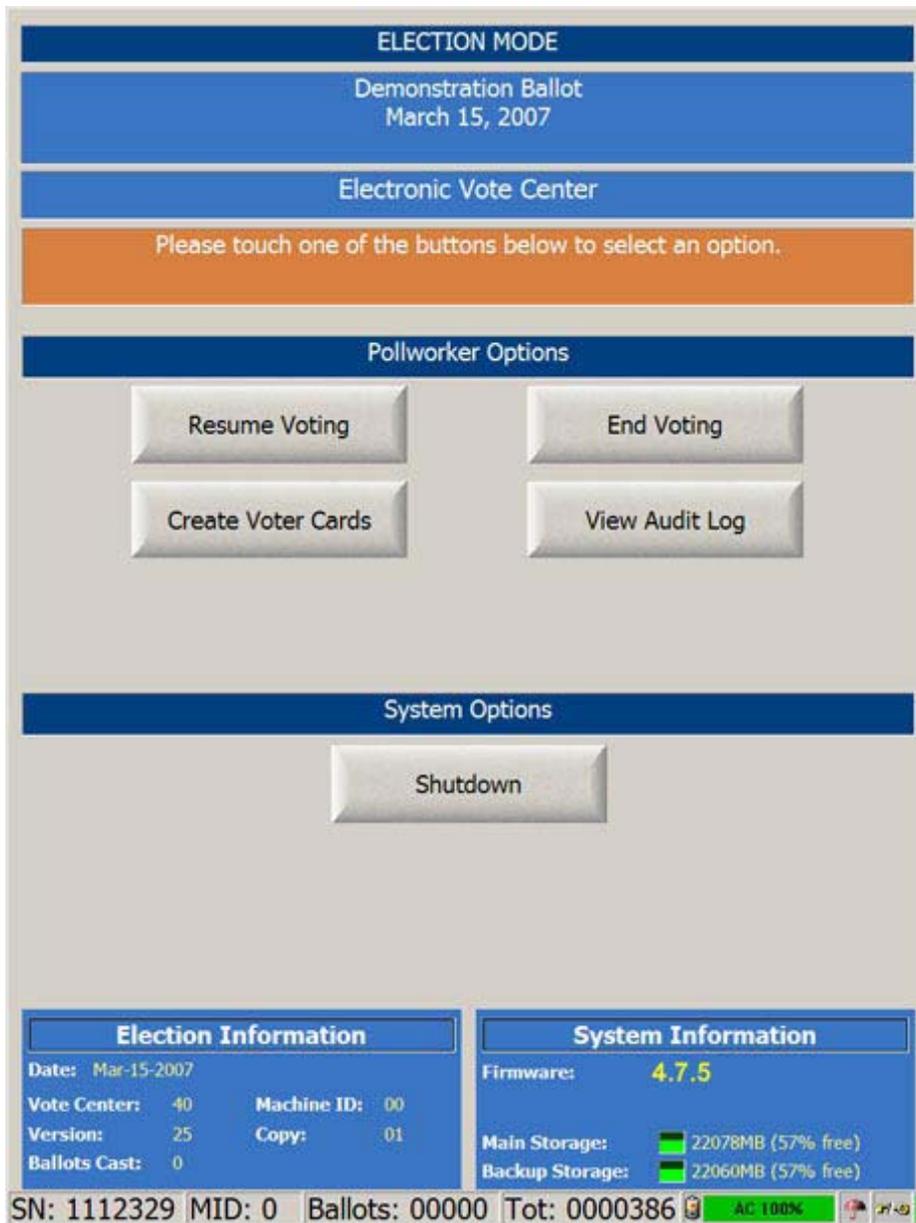


Figure 2-12: BallotStation – Election Mode

One of the buttons that can be accessed from the Pollworker menu is **View Audit Log**: Use this button to view the AccuVote-TSX Audit Log. All election related operations are logged to the Audit Log. When an installed memory card has been programmed with election data, system operations are logged to an Audit Log stored on both the memory card and the unit.