



COUNTY OF HUMBOLDT

AGENDA ITEM NO.

For the meeting of: January 13, 2009

Date: January 6, 2009

To: Board of Supervisors

From: Carolyn Crnich, Registrar of Voters

Subject: Voting Modernization Project Plan Phase II

RECOMMENDATION(S):

That the Board of Supervisors approve the attached Project Plan, Phase II to allow for the purchase of the system with Prop. 41 funds which will be matched with HAVA funds, and approve the implementation of the Hart InterCivic eScan as the County's primary voting system.

SOURCE OF FUNDING: Voting Modernization Funds (Prop. 41) and HAVA funds

DISCUSSION: Your approval of this Project Plan will allow the department to move forward with the applications for funding under Proposition 41 and the Help America Vote Act (HAVA). Using the funds available to us which are administered by the Secretary of State, there will be no cost to the County General Fund for these improvements. The Premier AccuVote system has been in use in Humboldt County since 1995. Increasing service and maintenance costs have caused us to review the entire system and consider other alternatives. In 2006 your Board approved the purchase of the Hart InterCivic eSlate system to assure that we met the accessibility deadlines in the Help America Vote Act.

Prepared by *Carolyn Crnich*

CAO Approval *Phillip Smith Hayes*

REVIEW: Auditor _____ County Counsel *JC* Personnel _____ Risk Manager _____ Other _____

TYPE OF ITEM:
___ Consent
___ Departmental
___ Public Hearing
___ Other _____

BOARD OF SUPERVISORS, COUNTY OF HUMBOLDT
Upon motion of Supervisor
Seconded by Supervisor
And unanimously carried by those members present,
The Board hereby adopts the recommended action
contained in this report.

PREVIOUS ACTION/REFERRAL:

Board Order No. _____

Meeting of: _____

Dated: _____
Kathy Hayes, Clerk of the Board

By: _____

Now in use for six elections, they have proven durable and reliable; however, their use has necessitated the creation of each election twice; once on the Hart BOSS system and once on the Premier GEMS system. This duplication of effort is not a prudent use of staff time and will be eliminated with the use of an integrated system (Hart InterCivic) rather than the current Premier/Hart InterCivic hybrid. Humboldt County is currently the only county in California using this combination of systems/vendors. The Hart InterCivic system has been certified for use in California by the Secretary of State.

FINANCIAL IMPACT: Because the cost of the new system will be covered by the above mentioned funds, there will be no impact to the County General Fund. A savings in staff overtime will be realized by the elimination of duplicate programming. Working with Secretary of State's staff, a specific financial plan will be developed using Voting Modernization Bond (Prop 41) and HAVA funds to cover the purchase of the proposed equipment and services. Both of these funding sources are administered by the Secretary of State. Because of the current fiscal crisis in the State of California, the voting Modernization Bond funds designated to cover this project were frozen by the State Treasurer on December 19, 2008. We will return to your Board for change order and funding plan approval once the funding plan is developed and approved by the Secretary of State. The delay in obtaining these funds should not impact the approval of the concept of this plan.

OTHER AGENCY INVOLVEMENT: California Secretary of State

ALTERNATIVES TO STAFF RECOMMENDATIONS: Do not proceed with the acquisition of the Hart InterCivic eScan system and continue to use the Premier AccuVote and GEMS systems and the Hart InterCivic eSlate Disabled Accessible Units for voters with disabilities.

ATTACHMENTS: Voting Modernization Project Plan Phase II
Certification of Hart InterCivic system by Secretary of State

Humboldt County, California

**Voting Modernization
Project Plan**

Phase II

November 3, 2008

Carolyn Cnich,
Registrar of Voters

3033 H Street
Eureka, CA 95501

(707)445-7678

Section 1 – Executive Summary

Anticipating a nationwide migration, Humboldt County in 1995 changed from a Votomatic punch card voting system to Global Election Systems AccuVote Optical Scan system (which was acquired by Diebold Election Systems, Inc. and is now known as Premier AccuVote-OS). After Proposition 41, the Voting Modernization Bond Act of 2002, was passed by the voters and after Congress passed the Help America Vote Act (HAVA), we began researching HAVA-compliant alternatives to the AccuVote-OS system.

While we had hoped to maintain this paper-ballot based system by implementing the Vote-PAD system, that system failed to meet certification standards, so we moved forward researching DRE systems that would meet the needs of the disabled voters of this community, provide a usable, reliable system, and meet the deadlines for accessibility required by HAVA. Our Elections Advisory Committee, a citizens group that meets monthly to study elections issues on a non-partisan basis, did extensive research into the equipment available to meet our needs and the HAVA requirements. The Hart InterCivic eSlate was found to be the best solution and 58 Disabled Accessible Devices were deployed for the November, 2006 election.

Working with Hart InterCivic has proven to be a very positive relationship. The programming for elections is much more streamlined and user friendly than the GEMS system still in use for the majority of Humboldt County Voters. But the combined Premier/Hart system has caused a huge increase in workload by necessitating the creation of each election in both Premier and Hart systems.

Because the AccuVote equipment was purchased in 1995, it is reaching the end of its useful life and we are seeing increased maintenance costs. It is therefore requested that this plan be approved to acquire the Hart InterCivic eScan optical scan equipment to replace the existing Premier AccuVote and GEMS systems.

Because there is not currently an election planned until November, 2009, this is the perfect time to implement a new system, allowing time for staff training as well as poll worker and voter training. Perhaps the most critical aspect of such implementation is that it will streamline staff time by making it possible to program each election only once for one homogenized system, but it will also allow for improved accessibility, security, and transparency.

Section 2 – Overall Voting System Modernization Strategy

A. What steps have you taken to determining the voting system under consideration is the appropriate system for your county?

In preparation for the impending deadlines of HAVA, the Humboldt County Board of Supervisors chartered the Humboldt Elections Advisory Committee in 2005 with the mission of studying all issues effecting local elections. This is a non-partisan group that has done extensive study in various voting systems and practices that could make our elections as transparent as possible while following the letter of State and Federal law. Their first task was to research various options for accessibility to meet the requirements of HAVA. It was determined that the best option for this county and our voters with disabilities would be the VotePAD, a system that did not pass the scrutiny of the Secretary of State's certification program.

Our next choice was the Hart InterCivic eSlate Disabled Accessible Unit (eSlate DAU). While the system was much more costly than the VotePAD, it had the obvious advantage of greater accessibility and greater ease of election programming, particularly in the area of recording the audible ballot for voters with vision impairment. It also offers greater reporting capabilities. Additionally, the eSlate DAU has proven to be a user friendly, reliable, and durable system.

But the programming of two separate and diverse systems to accomplish the necessary tasks of an election while providing the required accessibility actually amounts to programming each election twice on two separate systems. Such a duplication of effort is not an efficient use of resources. Additionally, considering the age of the current optical scan system, the number of instruments needing to be returned to the vendor for service and repair after each election increases with every use. Further, the service and maintenance cost is increasing with each election.

For these reasons, it is appropriate for this County to move forward with replacing the current optical scan system with a newer, more reliable system that would work in concert with our more recently purchased accessible equipment. While the Hart InterCivic eSlate system has been certified to a level that would allow for multiple instruments in each polling place, it is our desire to maintain the paper ballot as Humboldt County's primary voting system and thus the eScans would only be deployed at a rate of one to two per polling place, depending on the number of precincts in each polling place.

B. How will this new system be implemented? Will it be launched completely in one election or phased in during the coming election cycle?

The addition of precinct level and central count digital scan units represents a second phase of implementation of a completely accessible system. The first phase of the project was the aforementioned implementation of the Hart InterCivic DAU units in each polling place to meet the accessibility requirements of HAVA. This proposal is intended to complete our system under one vendor for a unified election system.

Because there is currently no county-wide election scheduled until November, 2009, full implementation of the system will be possible before the next election.

The following steps will be followed to assure a smooth transition:

- Acceptance and testing of all units. This phase will familiarize staff with the equipment and software and assure that all equipment and software is in order before acceptance
- Design space in a new location that will house the Elections Department in a more central, convenient location closer to other local administrative centers. This design will include enhanced security, storage and workspace.
- Train staff on use and maintenance of software and hardware. Enhanced reporting and security will be a part of the training provided by the vendor to assure that staff is aware of the features available to them in auditing and reporting functions. Such training will include a mock election.
- We will work with volunteer groups to improve and refine our poll worker training and define logistical procedures that will allow for improved deployment and return of equipment during an election.
- We will pursue certification as a Ballot Finisher in order to avail ourselves of the "Ballot Now" feature offered by the Hart system. This feature will streamline ballot distribution of vote-by-mail-ballots requested in office, eliminating the possibility of a voter being issued an incorrect ballot and greatly cutting down on printing costs as well as the waste of ballots. With the ability to print additional ballots in-house, we will eliminate the possibility of running out of ballots at any precinct during an election.
- Demonstrate the ballot review capabilities of Ballot Now which allows for the public review of ballots for which a decision must be made regarding voter intent or the validity of write-in votes. This is a significant step forward in the area of transparency of elections, a matter of great concern to the Elections Advisory Committee.

C. How will this implementation affect voters and poll workers?

Voters

Voters will notice a change in the appearance of the paper ballot. The rectangular voting opportunities and a bolder type face will provide for more 'readability'. Another difference the voters will appreciate is the larger screen on the eScan. The process of voting, marking a paper ballot, placing it into a secrecy sleeve and feeding it into the counting device will seem very similar to past voting experiences. But the machine will advise them in simple language of errors (overvotes and undervotes) and in which race the error occurred and instruct them on how to correct it or have the ballot counted as it is marked. This avoids the possible invasion of the voter's privacy when a poll worker has to interpret the message on the current equipment and assist the voter in overcoming an error.

Section 3 – Project Plan Summary

Project Objectives

Our primary objective is to provide all voters with the most accessible, secure, and reliable voting experience possible while complying with HAVA and state law regarding accessibility and using the resources available to us in a responsible and efficient manner.

A. What are the steps (or phases) your county will take to implement this new voting system? What resources will be allocated to implement this project?

Project Phases

Phase one of this project involved adding accessible voting devices to our existing paper ballot system. This has been accomplished with the addition of the Hart InterCivic eSlate DAU to our Premier AccuVote OS system.

Phase two is to move to a fully integrated system where the paper ballot is still the primary voting device. This will move us away from a hybrid system of one vendor's accessible voting devices and another vendor's optical scan system.

Phase three of this plan involves training of staff, poll workers and voters on the use of the system. Staff training will be provided by the vendor. Staff will then develop training plans for poll workers and outreach plans for voters.

Any further phases of this plan will be a continuation of the original objectives stated above that may become apparent with the implementation of phases two and three.

Resources

We will use Prop 41 and HAVA 301 funds for system acquisition and vendor support. All Elections Staff will be involved with the project as well as County Information Technology staff.

B. How much vendor support will be made available to your county under your contract?

Because the contract for the eSlate DAU phase of this project included ample service and support credits, we will continue to draw on those credits for the completion of this phase of the project.

C. What type of controls (or checks) is in place to make sure that your Project Plan is progressing properly?

Phase One of the Project was driven by the HAVA deadlines for implementation of accessible voting equipment. To make sure the project stayed focused and on course, charts and timetables were developed. For this phase of the project, similar timetables will be developed but not driven by the specific deadline of an election. Benchmarks will be set to assure that all testing (including a mock election) and training will be accomplished within four months of delivery of equipment. Setting a goal of four months will allow us to develop a mock election for training and testing purposes within realistic timeframes. This will also assure that, should a special election be called before the next scheduled election (November 2009), we will be prepared to stage such a special election efficiently and confidently.

D. Please provide a comprehensive "Accessibility Plan" on how your county's new voting system complies with state and federal law. How is your county going to comply with the requirements of AB 2525 (Jackson), Chapter # 950, and Statutes of 2002?

The proposed system was conditionally certified by the Secretary of State on December 6, 2007 and is fully compliant with the federal and state law.

We are offering voters both DRE and optical scan ballots. We will continue to provide paper ballots to disabled voters who prefer to vote in that way. We have booths accessible to voters in wheelchairs and we will continue to supply precinct boards with ballot magnifiers, voting pen grip adapters, instructions in large type, and we will provide curbside and assisted voting.

We have worked with local disability support groups to make our ballot materials available to visually impaired voters and will continue to do so. Our outreach has been successful. Although a lack of complaints is not necessarily an indication of success, we have had no complaints about our eSlate deployment or strategy.

Section 4 – Project Schedule

Milestones, Hardware/software Acquisition and Implementation Dates

Once the hardware is delivered, a date will be fixed for our mock election (Testing and Training Election). The "E-" dates below will be fixed with the establishment of that date.

- E-70 Hart delivers eScan system
- E-69 to E-55 Acceptance testing of equipment
- E-54 to E-44 Staff training on equipment use, maintenance and care
- E-45 to E-43 Staff programs Testing and Training Election
- E-40 Finish election programming, testing and installation of memory cards
- E-40 to E-35 Develop poll worker training materials
- E-35 to E-20 Print training materials for poll workers and publish same to Elections website.
- E-25 Begin voter outreach with media assistance to recruit volunteers for participation in Testing and Training election
- E-17 to E-14 Train poll workers
- E-13 to E-12 Train election day rovers (field technicians)
- E-2 Deploy DAU and eScans to inspectors
- E Testing and Training Election Day (to be determined as described above)
- E+ 1 to E+2 prepare reports from election with support and instruction of Hart InterCivic using formats prescribed by Secretary of State
- E+3 Meet with staff and poll workers to consider practices and procedures of Testing and Training Election to determine where improvements can be made
- E+4 and continuing: refine procedures and plans for future elections

State of California



SECRETARY OF STATE

WITHDRAWAL OF APPROVAL OF HART INTERCIVIC SYSTEM 6.2.1 DRE & OPTICAL SCAN VOTING SYSTEM AND CONDITIONAL RE-APPROVAL OF USE OF HART INTERCIVIC SYSTEM 6.2.1 DRE & OPTICAL SCAN VOTING SYSTEM (December 6, 2007 Revision)

Whereas, pursuant to Elections Code section 19201, no voting system, in whole or in part, may be used unless it has received the approval of the Secretary of State; and

Whereas, Elections Code section 19222 requires that I, as Secretary of State for the State of California, conduct periodic reviews of voting systems to determine if they are defective, obsolete, or otherwise unacceptable; and

Whereas, at my inauguration as Secretary of State on January 8, 2007, I announced my intention to conduct a top-to-bottom review of voting systems approved for use in California; and

Whereas, on March 22, 2007, I circulated for public comment draft criteria for a review of voting systems approved for use in California, covering system security issues, access for voters with disabilities, access for minority language voters, and usability for elections officials and poll workers; and

Whereas, pursuant to my statutory obligations, I have undertaken such a review of voting systems approved for use in California, including the Hart Intercivic System 6.2.1 voting system, pursuant to a contract with the Regents of the University of California and conducted by experts selected and supervised by principal investigators from the computer science faculties of the Berkeley and Davis campuses, to determine if the voting systems are defective, obsolete, or otherwise unacceptable for use in the February 5, 2008, Presidential Primary Election and subsequent elections in California; and

Whereas, the study was completed on July 20, 2007, following which the expert reviewers delivered their written reports on their findings and methodology; and

Whereas, the expert reviewers found that the quality of the 2002 Voting System Standards (VSS) to which each of the three systems in their study were certified is inadequate, and noted further that questions have been raised about the effectiveness of the testing; for example, Ciber, Inc., a testing laboratory involved in testing of voting systems under the 2002 VSS, has been denied interim accreditation for testing voting systems by the Federal Election Assistance Commission after finding that Ciber "was not following its quality-control procedures and could not document that it was conducting all the required tests"; and

Whereas, the expert reviewers demonstrated that the physical and technological security mechanisms provided by the vendors for each of the voting systems analyzed were inadequate to ensure accuracy and integrity of the election results and of the systems that provide those results; and

Whereas, the expert reviewers reported that all of the voting systems studied contain serious design flaws that have led directly to specific vulnerabilities, which attackers could exploit to affect election outcomes; and

Whereas, the Hart Source Code Review Team found that the Hart voting system contains design features that can be used in a fashion for which those design features were not intended, including network interfaces that are not secured against direct attack; and

Whereas, the Hart Source Code Review Team found that the Hart voting system's software fails to check the correctness of inputs from other Hart voting system components and uses those inputs in unsafe ways, potentially enabling an attacker to use voting system components to reprogram voting system units throughout the county with malicious code that would affect a subsequent election; and

Whereas, the Hart Source Code Review Team found that the Hart voting system exhibits a notable lack of the use of cryptographic security protocols to secure network communications, and where cryptography is used, a single countywide symmetric key is used that could allow a person to forge ballot information and election results in multiple polling locations; and

Whereas, the Hart Source Code Review Team found that the Hart voting system allows raw ballot records and other information to be used to reconstruct how each voter voted, potentially compromising the secrecy of the ballot; and

Whereas, the Hart Source Code Review Team found that many attacks are hard to detect and correct, defying development and implementation of simple, effective countermeasures; and

Whereas, the Hart Red Team that conducted penetration testing of the Hart voting system discovered multiple vulnerabilities; and

Whereas, on non-polling place components of the voting system that run on a Windows platform, Hart Red Team members located an undisclosed database user name and password and also manually bypassed Hart software security settings so they could run the Hart software in a standard Windows desktop environment, a possible vector for unauthorized access to the voting system's databases; and

Whereas, Hart Red Team members determined that the Hart voting system software fails to check the correctness of inputs from other Hart voting system components; and

Whereas, Hart Red Team members were able to access device-level menus on the Hart eScan precinct-based optical scan unit that should have been locked with passwords, which could allow access for altering voting system configuration settings; and

Whereas, Hart Red Team members confirmed findings from previous studies that allowed malicious actions to be performed on the Hart eScan precinct-based optical scan unit, including altering vote totals, using tools commonly found in an office; and

Whereas, Hart Red Team members were able to demonstrate the ability, after the close of the polls, to use a laptop computer to tamper with a Mobile Ballot Box memory device used to record votes cast on the eSlate direct recording electronic voting device, an attack that, if undetected during the tampering, could alter vote totals in a manner not detected by technological safeguards but detectable in a manual recount; and

Whereas, Hart Red Team members found that the Hart voting system allows for remote eavesdropping and capture of the audio narration of a ballot (a feature designed for use by voters with disabilities), potentially violating the secrecy of the ballot; and

Whereas, on July 30, 2007, a duly noticed public hearing was held to give interested persons an opportunity to express their views regarding the review of various voting systems, including the Hart Intercivic System 6.2.1 voting system; at this hearing, approximately 60 individuals testified; many more submitted comments by letter, facsimile transmission, and electronic mail; and

Whereas, pursuant to Elections Code section 19222, I, as Secretary of State, am authorized to withdraw approval previously granted of any voting system or part of a voting system if I determine that voting system or any part of that voting system to be defective or otherwise unacceptable; and

Whereas, I have reviewed the Hart Intercivic System 6.2.1 voting system and I have reviewed and considered several reports regarding the use of this voting system; the public testimony presented at the duly noticed public hearing held on July 30, 2007, and the comments submitted by letter, facsimile transmission, and electronic mail; and

Whereas, pursuant to Elections Code section 19222, six months' notice must be given before withdrawing approval previously granted of any voting system or part of a voting

system unless I, as Secretary of State, for good cause shown, make a determination that a shorter period is necessary; and

Whereas, pursuant to Elections Code section 19222, any withdrawal by the Secretary of State of the previous approval of a voting system or part of a voting system is not effective as to any election conducted within six months of that withdrawal; now

Therefore, I, Debra Bowen, Secretary of State for the State of California, find and determine, pursuant to Division 19 of the Elections Code, as follows:

For the reasons set forth above, the Hart Intercivic System 6.2.1 voting system, comprised of JBC, version 4.3.1, eSlate/DAU, version 4.2.13, eScan, version 1.3.14, VBO, version 1.8.3, eCM Manager, version 1.1.7, Ballot Now software, version 3.3.11, BOSS software, version 4.3.13, Rally software, version 2.3.7, Tally software, version 4.3.10, and SERVO, version 4.2.10, which was previously approved, is found and determined to be defective or unacceptable and its certification and approval for use in subsequent elections in California is withdrawn effective August 3, 2007, except as specifically provided below.

1. Before any use in the February 5, 2008, Presidential primary election, jurisdictions must reinstall all software and firmware (including reformatting all hard disk drives and reinstalling the operating system where applicable) on all election management system servers and workstations, voting devices and hardware components of the voting system. Voting system application software must be reinstalled using the currently approved version obtained directly from the federal testing laboratory or the Secretary of State.
2. Within 30 days of the original issuance of this document on August 3, 2007, the vendor must present a plan and jurisdiction Use Procedures to the Secretary of State for approval that will prevent future viral propagation of malicious software from one system component to another, such as from a voting system component located in one precinct to voting system components located in other precincts. The plan and Use Procedures must incorporate, or employ methods at least as effective as, a configuration of parallel central election management systems separated by an "air-gap" where (1) a permanent central system known to be running unaltered, certified software and firmware is used solely to define elections and program voting equipment and memory cards, (2) a physically-isolated duplicate system, reformatted after every election to guard against the possibility of infection, is used solely to read memory cards containing vote results, accumulate and tabulate those results and produce reports, and (3) a separate computer dedicated solely to this purpose is used to reformat all memory devices before they are connected to the permanent system again. (This "airgap" model was proposed by the Source Code Review Team that reviewed the Diebold Election Systems, Inc., GEMS 1.18.24 voting system. Further details concerning the model are provided in Section 6.10 of the Source Code Review of the Diebold Voting System, dated July 20, 2007, and available on the Secretary of

State website at http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf.)

The vendor's plan must prohibit the installation of TALLY and SERVO on the same computer. The vendor's plan must also require each SERVO computer to be rebooted from a write-once CD-ROM or read-only flash drive containing the trusted build of SERVO following each connection of an eSlate or JBC device to the SERVO computer and prior to connection of another eSlate or JBC device to the SERVO computer.

The vendor's plan must require jurisdictions that use more than one eSlate per precinct to permanently assign each precinct a set of JBC and eSlate devices, identified by serial number, for use in all elections, taking into account equipment replacement needs and precinct consolidations.

3. Within 30 days of the original issuance of this document on August 3, 2007, the vendor must submit to the Secretary of State for approval specifications for the hardware and operating system platform that must be used for all applicable components of the voting system. The vendor must identify the requirements for "hardening" the configuration of that platform, including, but not limited to:
 - BIOS configuration;
 - Identification of essential services that are required and non-essential services that must be disabled;
 - Identification of essential ports that are required and non-essential ports that must be disabled and, if feasible, removed or physically blocked;
 - Audit logging configuration;
 - Definition of user security roles and associated permissions to assure all users have only the minimum required permissions for their role;
 - Password policies, including password strength, expiration, and maximum attempts, along with all related user account control settings; and
 - All utilities and software applications, with specifications for their installation, configuration and use, that are necessary for operation of the voting system (e.g., security software, data compression utilities, Adobe Acrobat, etc.).

The vendor must identify automated mechanisms for jurisdictions to confirm and document that their system has been configured to these standards, and that all updatable components are the approved version and level. The vendor must provide full instructions for the use of these mechanisms, including expected results.

4. Immediately after any repair or modification of any voting system component that requires opening the housing, the integrity of the firmware and/or software must be verified using the automated mechanisms described above, or all software must be reinstalled by the jurisdiction from a read-only version of the approved firmware and/or software supplied directly by the federal testing laboratory or Secretary of State before the equipment can be put back into service.

5. Jurisdictions are prohibited from installing any software applications or utilities on any component of the voting system that have not been identified by the vendor and approved by the Secretary of State.
6. Within 30 days of the original issuance of this document on August 3, 2007, the vendor must develop and submit to the Secretary of State for approval, a plan and procedures for timely identification of required security updates (e.g., operating system security patches, security software updates, etc), vendor testing of the updates, and secure distribution and application of vendor-approved security updates.
7. Within 45 days of the original issuance of this document on August 3, 2007, the vendor, working with elections officials, must develop and submit to the Secretary of State for approval, requirements and use procedures for operating and maintaining the physical and logical security of the system, including, but not limited to:
 - Physical security and access to the system and all components;
 - Network security;
 - Data security (including data backup requirements and procedures); and
 - Separation of roles and responsibilities for jurisdiction personnel.
8. No network connection to any device not directly used and necessary for voting system functions may be established. Communication by or with any component of the voting system by wireless or modem transmission is prohibited at any time. No component of the voting system, or any device with network connectivity to the voting system, may be connected to the Internet, directly or indirectly, at any time.
9. Within 45 days of the original issuance of this document on August 3, 2007, the vendor, working with elections officials, must develop and submit to the Secretary of State for approval, detailed requirements and use procedures for programming, pre- and post-election logic and accuracy testing, transporting and operating voting equipment that will prevent or detect unauthorized access to or modification of any component of the voting system, including, but not limited to:
 - Chain of custody controls and signature-verified documentation;
 - Requirements for secure interim storage of any system component; and
 - Employment of mechanisms to detect unauthorized access to the equipment.

Following meetings with vendor and county representatives in the period from September 28, 2007, through October 5, 2007, the Secretary of State has determined that, at a minimum, the Use Procedures must require the jurisdiction to secure all voting system components in one or more uniquely serialized, tamper-evident container(s) before the jurisdiction transfers them to the custody of an Inspector, other poll worker, drayage company or other intermediary, or before jurisdiction personnel deliver them to a secure polling place or secure satellite distribution facility, as the case may be. Transportation of voting system components to the custody of an Inspector, other poll worker, drayage company or other intermediary, secure polling place, or secure satellite distribution facility shall not occur earlier than 10 calendar

days prior to Election Day. Electronic components of a voting system not transported back to the jurisdiction headquarters on election night must be secured in one or more uniquely serialized, tamper-evident container(s) and placed in secured storage. The use procedures must impose the same requirements for signed logging of the inspection of security containers and the removal and return of voting system components to security containers that apply to security seals and locks on the voting system components themselves. The following are examples of acceptable tamper-evident containers:

- A uniquely serialized, sealed banker's bag;
- A zippered nylon or canvass bag or case on which the zipper(s) that prevent access to the voting system component(s) inside are kept closed by a uniquely serialized, tamper-evident lock; or
- A hard lid that blocks access to all doors, ports or other points of access to the inside of the voting system component(s) and that is held in place by a latch or latches closed with a uniquely serialized, tamper-evident lock or locks.

The Use Procedures must also require a minimum of two elections officials or poll workers to perform or directly observe critical security processes, such as sealing and locking equipment for transport, conducting logic and accuracy testing, verifying the integrity and authenticity of security locks and seals, setting up voting equipment, opening the polls, closing the polls and printing results.

10. Where application of tamper-evident seals directly to a system component is required to detect unauthorized access to the component, those seals must be serialized and the vendor must specify in each instance the type of the seal to be used and the exact placement of that seal using photographs.
11. Upon request, members of the public must be permitted to observe and inspect, without physical contact, the integrity of all externally visible security seals used to secure voting equipment in a time and manner that does not interfere with the conduct of the election or the privacy of any voter.
12. Where voting equipment is used to record and tabulate vote results in a polling place, upon close of the polls, the poll workers are required to print two copies of the accumulated vote results and one audit log from each JBC or eScan. Each poll worker must sign every copy. One copy of the vote results from each device must be publicly posted outside the polling place. The second copy, along with the audit log, must be included with the official election material that is returned to the jurisdiction headquarters on election night.
13. No poll worker or other person may record the time at which or the order in which voters vote in a polling place.
14. Poll workers are not permitted to have access to any VBO audit records, nor may they participate in any audits or recounts involving VBO audit records. Poll workers may

participate in audits involving VBO audit records from a precinct other than the one in which they were a poll worker.

15. Within 60 days of the original issuance of this document on August 3, 2007, the vendor, working with elections officials, must develop and submit to the Secretary of State for approval, specific detailed requirements and use procedures for vote results auditing and reconciliation, review of audit logs and retention of election documentation to validate vote results and detect unauthorized manipulation of vote results, including, but not limited to:
 - Precinct level ballot accounting;
 - Identification of abnormal voting patterns on VBO audit trails; and
 - Reconciliation of variances between electronic and manual audit vote results.
16. Any post-election auditing requirements imposed as a condition of this certification shall be paid for by the vendor. Elections officials are required to conduct the audits and the vendor is required to reimburse the jurisdiction.
17. After consultation with elections officials, the Secretary of State shall establish additional post-election manual count auditing requirements, including:
 - Increased manual count sample sizes for close races, based on an adjustable sample model, where the size of the initial random sample depends on a number of factors, including the apparent margin of victory, the number of precincts, the number of ballots cast in each precinct, and a desired confidence level that the winner of the election has been called correctly. In establishing sampling requirements for close races, the Secretary of State may impose a specific sampling threshold for a given 10 vote differential or percentage of the margin of victory, taking into account the number of electors and the number and size of precincts in the race;
 - Escalation requirements for expanding the manual count to additional precincts when variances are found; and
 - Procedures to increase transparency and effectiveness of post election manual count audits.

Elections officials must comply with these requirements as set forth by the Secretary of State in the document entitled "Post-Election Manual Tally Requirements" and any successor document. The vendor shall reference compliance with the "Post-Election Manual Tally Requirements" in its Use Procedures for the voting system

18. Each polling place must be equipped with a method or log in a format specified by the Secretary of State after consultation with the elections officials to record all problems and issues with the voting equipment in the polling place as reported by voters or observed by poll workers. Such records must include the following information for each event:
 - Date and time of occurrence;
 - Voter involved, if any;
 - Equipment involved;

- Brief description of occurrence;
- Actions taken to resolve issue, if any; and
- Elections official(s) who observed and/or recorded the event.

All such event logs or reports must be made available to the public for inspection and review upon request. Prior to or concurrent with the certification of the election, the elections official must submit a report to the Secretary of State of all reported problems experienced with the voting system and identifying the actions taken, if any, to resolve the issues.

19. Training of poll workers must include the following:

- Secure storage of voting equipment while in the poll worker's possession;
- Chain-of-custody procedures required for voting equipment and polling place supplies;
- Seal placement and procedures for verification of seal integrity;
- Placement and observation of voting equipment;
- Observation of activity that could indicate tampering or an attempt at tampering;
- The Voter Bill of Rights set forth in section 2300 of the Elections Code;
- The purpose served by the Voter Verified Paper Audit Trail (VVPAT), the importance of its use by voters, and how to handle problems such as paper jams;
- How to ensure, when required, that a minimum of five voters vote on each DRE in a polling place;
- The public right to inspect voting equipment and security seals, and how to handle requests for such inspection;
- How to handle equipment failure or lack of sufficient paper ballots in a polling place and how to ensure continuity of the election in the event of such a failure; and
- How to properly log all events and issues related to voting equipment in the polling place, including voter complaints of malfunctioning equipment.

20. Elections officials must develop appropriate security procedures for use when representatives of qualified political parties and bona fide associations of citizens and media associations, pursuant to their rights under Elections Code section 15004, check and review the preparation and operation of vote tabulating devices and attend any or all phases of the election. The security procedures must permit representatives to observe at a legible distance the contents of the display on the vote tabulating computer or device. This requirement may be satisfied by positioning an additional display monitor or monitors in a manner that allows the representatives to read the contents displayed on the vote tabulating computer or device while also observing the vote tabulating computer or device and any person or persons operating the vote tabulating computer or device.

21. All voters voting on paper ballots in a polling place must be provided a privacy sleeve for their ballot and instructed on its use in accordance with Elections Code section 14272.

22. A warning must be posted in each voting booth stating that, pursuant to Elections Code sections 18564, 18565, 18566, 18567, 18568 and 18569, tampering with voting equipment or altering vote results constitutes a felony, punishable by imprisonment.
23. With respect to any piece of voting equipment for which the chain of custody has been compromised or for which the integrity of the tamper-evident seals has been compromised, the following actions must be taken:
- The chief elections official of the jurisdiction must be notified immediately;
 - The equipment must be removed from service immediately and replaced if possible;
 - Any votes cast on the device prior to its removal from service must be subject to a 100% manual tally, by the process described in Elections Code section 15360, as part of the official canvass. Notice to the public of this manual tally may be combined with the notice required by any other manual tally required in this order or by Elections Code section 15360;
 - Any memory card containing data from that device must be secured and retained for the full election retention period;
 - An image of all device software and firmware must be stored on write-once media and retained securely for the full election retention period; and
 - All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.
24. If a voting device experiences a fatal error from which it cannot recover gracefully (i.e., the error is not handled through the device's internal error handling procedures with or without user input), such that the device must be rebooted or the device reboots itself to restore operation, the following actions must be taken:
- The chief elections official of the jurisdiction must be notified immediately;
 - The equipment must be removed from service immediately and replaced as soon as possible;
 - Any votes cast on the device prior to its removal from service must be subject to a 100% manual tally, by the process described in Elections Code section 15360, over and above the normal manual tally conducted during the official canvass as defined in Elections Code section 336.5. Notice to the public of this manual tally may be combined with the notice required by any other manual tally required in this order or by Elections Code section 15360;
 - Any memory card containing data from that device must be secured and retained for the full election retention period;
 - An image of all device software and firmware must be stored on write-once media and retained securely for the full election retention period;
 - The vendor or jurisdiction shall provide an analysis of the cause of the failure;
 - Upon request by the Secretary of State, the vendor or jurisdiction shall retain the device for a reasonable period of time to permit forensic analysis; and
 - All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing

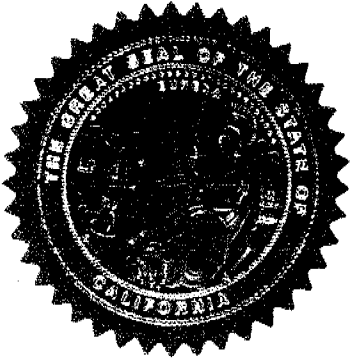
laboratory or the Secretary of State before the equipment is placed back into service.

25. The Secretary of State will review and finalize all plans, requirements and procedures submitted pursuant to the foregoing requirements above within thirty days of receipt. Upon approval, all such plans, requirements and procedures will automatically be incorporated into the official use procedures for the voting system, and will become binding upon all users of the system.
26. No substitution or modification of the voting system shall be made with respect to any component of the voting system, including the Use Procedures, until the Secretary of State has been notified in writing and has determined that the proposed change or modification does not impair the accuracy and efficiency of the voting system sufficient to require a re-examination and approval.
27. The Vendor developed utilities, Fusion, In-Fusion, Bravo and Trans, are specifically excluded from this certification.
28. The Secretary of State reserves the right, with reasonable notice to the vendor and to the jurisdictions using the voting system, to modify the Use Procedures used with the voting system and to impose additional requirements with respect to the use of the system if the Secretary of State determines that such modifications or additions are necessary to enhance the accuracy, reliability or security of any of the voting system. Such modifications or additions shall be deemed to be incorporated herein as if set forth in full.
29. Any jurisdiction using this voting system shall, prior to such use in each election, file with the California Secretary of State a copy of its Election Observer Panel plan.
30. The vendor agrees in writing to provide, and shall provide, to the Secretary of State, or to the Secretary of State's designee, within 30 days of the Secretary of State's demand for such, a working version of the voting system, including all hardware, firmware and software of the voting system, as well as the source code for any software or firmware contained in the voting system, including any commercial off the shelf software or firmware that is available and disclosable by the vendor, provided that the Secretary of State first commits to the vendor in writing to maintain the confidentiality of the contents of such voting system or source code so as to protect the proprietary interests of the vendor in such voting system or source code. The terms of the commitment to maintain confidentiality shall be determined solely by the Secretary of State, after consultation with the vendor. The voting system shall not be installed in any California jurisdiction until the vendor has signed such an agreement. Any reasonable costs associated with the review of the source code for any software or firmware contained in the voting system shall be born by the vendor.

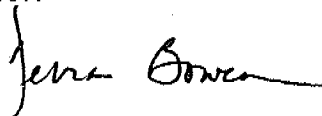
31. The Secretary of State reserves the right to monitor activities before, during and after the election at any precinct or registrar of voters' office, and may, at his or her discretion, conduct a random parallel monitoring test of voting equipment.
32. By order of the Secretary of State, voting systems certified for use in California shall comply with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. Further, voting systems shall also comply with all state and federal voting system guidelines, standards, regulations and requirements that derive authority from or are promulgated pursuant to and in furtherance of California Elections Code and the Help America Vote Act of 2002 or other applicable state or federal law when appropriate.
33. Voting system manufacturers or their agents shall assume full responsibility for any representation they make that a voting system complies with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. In the event such representation is determined to be false or misleading, voting system manufacturers or their agents shall be responsible for the cost of any upgrade, retrofit or replacement of any voting system or its component parts found to be necessary for certification or otherwise not in compliance.
34. Any voting system purchased with funds allocated by the Secretary of State's office shall meet all applicable state and federal standards, regulations and requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002.
35. The vendor must establish a California County User Group and hold at least one annual meeting where all California users and Secretary of State staff are invited to attend and review the system and ensure voter accessibility.
36. In addition to depositing the source code in an approved escrow facility, the vendor must deposit with the Secretary of State a copy of the system source code, binary executables and tools and documentation, to allow the complete and successful compilation and installation of a system in its production/operational environment with confirmation by a verification test by qualified personnel using only this content. The Secretary of State reserves the right to perform a full independent review of the source code at any time.
37. The vendor must provide printing specifications for paper ballots to the Secretary of State. The Secretary of State will certify printers to print ballots for this system based upon their demonstrated ability to do so. The vendor may not require exclusivity in

ballot printing and must cooperate fully in certification testing of ballots produced by other ballot printers.

38. Where circumstances require it, the Secretary of State may adjust or suspend any of the conditions of recertification for a vendor or a jurisdiction, as the Secretary of State deems prudent and necessary to facilitate successful election administration. Such adjustments or suspensions shall be deemed to be incorporated herein as if set forth in full.



IN WITNESS WHEREOF, I hereunto set my hand and affix the Great Seal of the State of California, this 6th day of December 2007.


DEBRA BOWEN
Secretary of State