

Brewer Voting Action Plan

May 3, 2005  www.azsos.gov

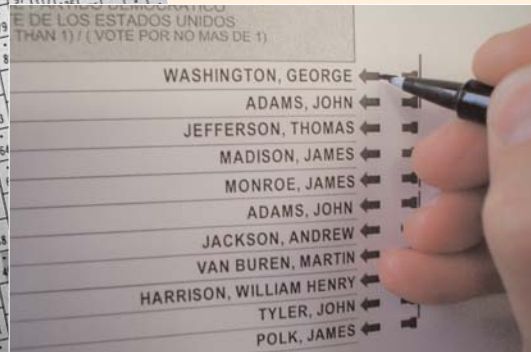
Arizona Secretary of State's Office

IMPROVING & BUILDING ELECTION ADMINISTRATION

MORE CONFIDENCE IN ARIZONA ELECTIONS



Janice K. Brewer
Secretary of State



 **APPROVED**

Janice K. Brewer

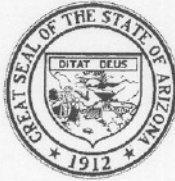


Election Services Division
1700 W. Washington St., 7th Fl.
Phoenix, Arizona 85007
602-542-8683
1-877-THE VOTE



INSIDE: Fair & Accurate Elections Secure Elections Paper Trails Shared Information Training & Education New Standards & Equipment

FINAL PLAN



JAN BREWER
SECRETARY OF STATE
STATE OF ARIZONA

May 3, 2005

Dear Arizonan:

In December 2003, I announced that I was leading a new effort to formulate a voting system action plan that would address statewide voting system and technology issues as part of my ongoing commitment to ensure integrity in our election process. After over a year of collecting data and input from the public and election administrators, I have completed the Brewer Voting Action Plan, which includes several comprehensive findings and recommendations. This is another major milestone in my efforts to improve election administration and build even more confidence in the accuracy and reliability of our election processes here in Arizona.

Over the past two years, my office has moved forward to ensure that all Arizonans are voting on equipment that minimizes the possibility of accidental overvotes and other voting controversies as discovered in the 2000 Presidential election in Florida. We adopted new voting system standards for all election workers to use as part of our State Procedures Manual. We also procured optical scan voting technology for those nine counties still using punch card voting systems, thus ridding our state of antiquated machines that previously may have led to "pregnant or hanging chads". In 2003, my office introduced the first requirement ever into law that requires voting equipment to receive full testing and certification by a federally accredited laboratory pursuant to the Help America Vote Act of 2002 (HAVA).

The Brewer Voting Action Plan is the result of a full analysis of Arizona's current voting technology, voting security systems, voting system certification procedures, and the general standards and operating procedures followed by our state and county election officials in administering Arizona's federal and state elections. I am proud to present the findings and recommendations from this comprehensive review.

The preliminary Brewer Plan was available for public comment starting on December 20, 2004 for a 30-day period. The Secretary of State's Office received many comments and suggestions that were carefully reviewed. Many of the suggestions have been incorporated into the final version of the Brewer Plan. In addition, Proposition 200 was passed by the Arizona voters at the November 2, 2004 general election and was proclaimed into law by the Governor on December 13, 2004. The United States Department of Justice precleared the new law on January 24, 2005. Some of the recommendations have been modified to include aspects of Proposition 200.

We have some of the most dedicated and honest election workers who continue to build public confidence, make certain that votes are properly counted, and ensure integrity in our election process. I remain highly confident that Arizona's statewide election process is as accurate and reliable as any jurisdiction in the country. I am confident that the Brewer Voting Action Plan will further improve Arizona's election process.

Sincerely

A handwritten signature in cursive script that reads "Janice K. Brewer".

Janice K. Brewer
Arizona Secretary of State

State Capitol: 1700 W. Washington Street, 7th Floor
Phoenix, Arizona 85007-2888
Telephone (602) 542-4285 Fax (602) 542-1575

Brewer Voting Action Plan

INTRODUCTION	2
BACKGROUND	3
EXECUTIVE SUMMARY	4
RECOMMENDATIONS	9
I. IMPROVE ELECTION PROCEDURES TO ENSURE FAIR AND ACCURATE ELECTIONS	9
II. INCREASE VOTING SYSTEM SECURITY PROCEDURES TO RAISE PUBLIC CONFIDENCE IN ELECTIONS	14
III. REQUIRE A VOTER VERIFIABLE PAPER BALLOT OR RECORD FOR ALL TYPES OF VOTING SYSTEMS USED IN ARIZONA	16
IV. INCREASE THE SHARING OF INFORMATION AND LESSONS LEARNED	19
V. PROVIDE FORMAL SECURITY AWARENESS INFORMATION, TRAINING, EDUCATION, AND PROCEDURES	21
VI. STRENGTHEN CURRENT STATE CERTIFICATION POLICIES AND STANDARDS FOR VOTING EQUIPMENT AND SOFTWARE TO INCREASE VERIFIABILITY AND TRANSPARENCY IN THE ELECTION PROCESS.	24
VII. IMPLEMENT STANDARDS AND RECOMMENDATIONS FROM THE ELECTION ASSISTANCE COMMISSION	27
VIII. MODERNIZE ELECTION EQUIPMENT AND SOFTWARE	28
IX. ENHANCE THE STATEWIDE VOTER REGISTRATION SYSTEM	30
APPENDIX - GARTNER ASSESSMENT OF ELECTION SYSTEMS REPORT	35

INTRODUCTION

On December 12, 2003, Secretary of State Jan Brewer announced the formulation of a new voting action plan as part of her ongoing commitment to maintain the integrity of Arizona's election process. Secretary Brewer is now pleased to present the *Brewer Voting Action Plan* (Brewer Plan).

This plan makes recommendations to improve election administration in Arizona and to ensure that the citizens of Arizona have the highest degree of confidence in the accuracy and reliability of our election process. The scope of the recommendations contained in the plan covers all federal and state elections under the jurisdiction of the Arizona Secretary of State's Office. Public input was sought before the plan was finalized.

The Secretary of State's Office conducted an intensive review of Arizona's election systems and processes in consultation with Gartner Consulting, one of the world's leading information technology research and advisory firms. Gartner was chosen because of its vast familiarity with the dynamics and developments in electronic voting systems and its expertise in election technology and the election procedures followed by other jurisdictions.

This plan is the result of a full analysis of Arizona's current voting technology, voting security systems, voting system certification procedures, and the general standards and operating procedures followed by our state and county election officials in administering Arizona's federal and state elections. The review revealed hundreds of important technical and practical suggestions for the State of Arizona to improve its voting systems, now and in the future.

Recommendations in the Brewer Plan are based in part on the review of the election systems and processes in Arizona and also incorporate communications and input from the county election administrators and the general public. A primary focus of this plan is to address the reliability and security concerns surrounding electronic or computer-based voting systems, commonly referred to as "touch screen" or direct recording electronic (DRE) devices.

Formulation of this plan included an analysis of recent studies and articles regarding election technology and security, correspondence and observations between vendors and staff, site surveys and focused interviews of county election officials that were conducted throughout the state. During this process, best practices from around the nation were identified through communication with other state and local jurisdictions regarding their certification and security processes, and a full evaluation was made of the hardware and software currently in use throughout Arizona.

The *Brewer Voting Action Plan* presents the first major review of Arizona's election processes in over a decade. The findings and recommendations in the plan represent the primary and most critical changes from this year-long assessment. This plan provides the state and county election officials with a detailed strategy and focuses on what priorities should be immediately implemented under the leadership of the Brewer Administration. In addition, the review identified other issues that will need to be considered and addressed in the future as our state continues to grow.

BACKGROUND

As a result of issues raised during the 2000 Federal Election, the processes in each state have been closely scrutinized. In response, Congress enacted the Help America Vote Act of 2002 (HAVA) on October 29, 2002. In addition, Arizona made several important changes to its election laws and procedures to implement HAVA and to assure Arizona's elections would continue to operate smoothly in the future. The mandates set forth in HAVA are designed for implementation over a period of several years. This plan sets forth recommendations that are designed to work in conjunction with the ongoing implementation of HAVA in addition to improving our state's overall voting procedures.

A primary feature of HAVA is the distribution of federal monies to upgrade each state's voting equipment. It also sets forth voting system standards to assure accuracy, mandates the creation of a statewide voter registration system, requires a provisional ballot process so voters can ascertain the disposition of their ballot, sets a deadline for states to provide independent access and confidentiality for voters with disabilities to vote on appropriate voting devices, and provides for the implementation of procedures that will protect each citizen's right to vote.

Shortly after HAVA was enacted, Secretary of State Jan Brewer published the *Arizona HAVA State Plan* that identified the priorities and specific steps the State of Arizona would take to address election reform and bring Arizona into compliance with HAVA. The HAVA plan was developed in conjunction with the State Planning Committee and was adopted unanimously from a group of state officials, legislative representatives, local officials, party representatives and individuals with special interests in improving access to the disabled. The HAVA plan called for the use of optical scan voting equipment in all 15 counties because it was proven technology with good audit capability. Secretary Brewer chose to have these machines ready for use in the 2004 elections rather than waiting until 2006 as permitted by HAVA. All 15 counties used this voting technology successfully during the 2004 elections.

Despite this success, perceived security issues surrounding electronic voting and other electoral processes persist. Under HAVA, every polling site must have a direct recording electronic (DRE) or other accessible voting device for the disabled in place before the 2006 federal elections. The Secretary of State's Office has begun identifying the business requirements, technological needs, and legal requirements of the state in procuring accessible voting devices for disabled persons by 2006. It is therefore necessary to address the security concerns associated with this technology as well as other potential security issues surrounding the entire electoral process in Arizona.

The disabled community was the driving force behind the passage of HAVA and its mandate for accessible voting machines at each polling site. The primary concern expressed by this community to Congress was the need to vote in private and without assistance. Some of the enthusiasm for DRE or "touch screen" voting devices was dampened when computer science experts and others raised concerns of mechanical failures and potential security threats from computer hackers. Additional questions also arose over the verifiability of votes cast, leading many states to shy away from these devices or require them to produce a paper ballot or record to allow the voter to verify his or her selections before the vote is officially cast.

Secretary Brewer believes touch screen voting systems can be used safely and effectively, but the ongoing nationwide controversies over this technology could ultimately force changes to existing federal standards. With so many unknowns in the future for touch screen systems, Secretary Brewer urged a cautious approach in meeting the federal mandates for accessibility. The completion of the year long review, along with the recommendations contained in the Brewer Plan, are timed to work with the *Arizona HAVA State Plan*.

The concerns surrounding voting systems and security have not been limited to DRE and touch screen voting devices. Consequently, this plan presents recommendations regarding other critical voting processes, including the manner in which the state certifies voting equipment, the manner in which the state follows security practices with respect to all computerized voting systems, the procedures followed at the polling places, the security surrounding the transportation and processing of ballots, poll worker training, and the statewide voter registration process. *The Brewer Voting Action Plan* provides important findings and recommendations to be used in improving these procedures and accomplishing the mandates set forth in HAVA.

EXECUTIVE SUMMARY

The Brewer Voting Action Plan outlines an overall strategy, identifies specific and important recommendations, and establishes a basic timeline to ensure proper security requirements for the entire Arizona electoral process. This plan was developed in response to concerns raised over security in voting equipment, and with the expectation that an in-depth analysis of current election procedures will improve our elections and further ensure the integrity of the voting process.

The election review conducted over the past year identified several findings, most of which are not unique to Arizona. The key findings are as follows:

- The 2000 Presidential Election raised awareness and skepticism of the election process.
- Not all county election procedures are clearly established, which can result in inconsistent application throughout the state.
- Elections are becoming more reliant on technology.
- The public is distrustful of the manner in which electronic voting machines tabulate and store votes.
- The public wants a voting system that allows them to verify their selections on paper.
- The disabled community desires to vote privately and without assistance.
- Strengthening the election security procedures will raise public confidence in the election process.

- The election process improves with the increased sharing of information between election officials, vendors, and interested parties.
- Properly trained poll workers are absolutely critical to the election process.
- The quality of election official training and poll worker training has a tremendous impact on the quality of the election.
- The policies, procedures and practices of election officials must continue to be evaluated and improved where necessary.
- State certification procedures for election equipment and software need to be more detailed.
- The Election Assistance Commission needs to provide standards and recommendations to election officials.
- The state and counties need to standardize and modernize election equipment and software.
- The processing of voter registration information, sharing of data between government agencies, and the maintenance of accurate voter registration information needs to be improved over time.

The primary recommendations of the *Brewer Voting Action Plan* are as follows:

I. Improve election procedures to ensure fair and accurate elections.

1. Implement procedures to verify transmitted election results for all elections once materials are returned from the precincts.
2. Establish contingency plans in the event that outside contractors are unable to perform their duties.
3. Establish minimum standards of emergency preparedness for all counties.
4. Strengthen laws, policies, and procedures concerning recounts and contested elections.
5. Clarify and enhance polling place procedures regarding physical set up, poll workers, and observers.
6. Improve logic and accuracy testing procedures.

II. Increase voting system security procedures to raise public confidence in the elections.

1. Implement minimum statewide standards and procedures for physical storage and transport of election machines and ballots.
2. Seek legislation to increase penalties for tampering with election equipment or software.
3. Implement minimum polling place security procedures to ensure no malicious tampering occurs with election equipment or software.
4. Implement procedures to ensure that proper security methods and practices are applied to all election system software and hardware.
5. Implement procedures to ensure that election systems are not connected to the Internet and that election equipment is used only for election purposes.

III. Require a voter verifiable paper ballot or record for all types of voting systems used in Arizona.

1. Optical Scan technology will remain the primary tabulation technology used in Arizona.
2. Any accessible voting device (DRE or touch screen voting machine) will be required to have a paper ballot or record that visually indicates all votes cast.

IV. Increase the sharing of information and lessons learned.

1. Establish semi-annual post election meetings of county and local election officials to identify and recommend voting system procedure improvements.
2. Increase the sharing of information among election officials using similar equipment by establishing user groups.
3. Implement a communication schedule with Arizona vendors of election systems to ensure compliance with Arizona policies and procedures.
4. Conduct public meetings to discuss election topics.

V. Provide formal security awareness information, training, education, and procedures.

1. Enhance election official training by expanding election curriculum and offering training to all county and local election personnel.
2. Enhance poll worker training guidelines.
3. Provide state funding for poll worker training.

4. Increase state funding for voter outreach to ensure the public is informed about election systems and procedures.

VI. Strengthen current state certification policies and standards for voting equipment and software to increase verifiability and transparency in the election process.

1. Require software and firmware source code be held in escrow.
2. Require all changes to voting systems used in Arizona be certified by the Secretary of State and national independent testing authorities for full functional and security testing.
3. Implement certification best practices learned from other states and the Election Assistance Commission.
4. Ensure that only certified software, hardware, and firmware are used in Arizona elections.
5. Post all certified election equipment and software on the Secretary of State Web site.
6. Seek legislation to allow the Secretary of State to grant conditional emergency certification when warranted.
7. Require county election officials to verify every election that only certified hardware, firmware, and software is in use.

VII. Implement standards and recommendations from the Election Assistance Commission (EAC).

1. Review and evaluate all recommendations and best practices set forth by the EAC.

VIII. Modernize election equipment and software.

1. Replace antiquated punch card voting machines with optical scan technology.
2. Provide accessible voting devices for voters with disabilities.
3. Continue to monitor the state of the election equipment industry.
4. Develop a statewide election equipment refresh policy.

IX. Enhance the statewide voter registration system.

1. Enhance the statewide voter registration system with improved processes and technology to ensure accurate voter registration rolls.
2. Enhance the ability of citizens to know the status of their provisional ballot.

3. Improve the accessibility for all citizens to the voter registration process.
4. Ensure that the statewide voter registration database is accessible to county voter registration officials.
5. Seek legislation to improve the quality of voter registration drives.

Arizona elections have run smoothly in the past. Arizona has also been a leader in implementing HAVA, and unlike the majority of states, Arizona chose not to ask for time waivers on the two largest sections of HAVA, replacing punch card voting machines and building a statewide voter registration list. Instead, Arizona implemented both of these mandates in time for the 2004 elections. The experiences gained from implementing these sections of HAVA have placed Arizona in a favorable position to continue to improve the election process throughout the state.

The preliminary Brewer Plan was available for public comment starting on December 20, 2004 for a 30-day period. The Secretary of State's Office received many comments and suggestions that were carefully reviewed. Many of the suggestions have been incorporated into the final version of the Brewer Plan. In addition, Proposition 200 was passed by the Arizona voters at the November 2, 2004 general election and was proclaimed into law by the Governor on December 13, 2004. The United States Department of Justice precleared the new law on January 24, 2005. Some of the recommendations have been modified to include aspects of Proposition 200.

Since the introduction of the preliminary plan, some implementation work has already begun. Several of the recommendations for statutory changes are contained in SB1342 that was signed into law by the Governor on April 19, 2005.

The Brewer Plan contains many recommendations that will require contributions from the entire election community to implement. Most of the recommendations are specific, but some need additional review to determine all of the details. Committees will be assembled to determine the specific steps to take on these recommendations. All of the recommendations will take hard work to implement. The timeline for completing most of the recommendations in the plan is the 2006 Federal Elections.

RECOMMENDATIONS

I. IMPROVE ELECTION PROCEDURES TO ENSURE FAIR AND ACCURATE ELECTIONS.

Arizona's election laws and procedures are set forth in Title 16 and 19 of the Arizona Revised Statutes. In addition, the *Secretary of State's Election Instruction and Procedures Manual* (Procedures Manual) identifies rules for obtaining the "maximum degree of correctness, impartiality, uniformity and efficiency on the procedures for early voting and voting, and of producing, distributing, collecting, counting, tabulating and storing ballots." This section of the Brewer Plan identifies several steps that should be taken to review Arizona's election laws and procedures to ensure that Arizona's elections continue to be conducted in a fair and accurate manner.

1. Implement procedures to verify transmitted election results for all elections once materials are returned from the precincts.

On election night most precinct results are communicated electronically through modems from the polling location to the counties' central site where results are tabulated. Computer experts have speculated that it would be theoretically possible for a hacker to somehow "hijack" this transmission and send false results. While this is a remote possibility, it is not considered to be a viable threat for several reasons.

First, the hacker would need to breach the built-in password security of the tabulation machine. Second, the hacker would need an extreme amount of inside information to accomplish this task, including information on internal precinct names and election database keys that change whenever the election database is modified. Third, the hacker would have to time his or her false transmission perfectly so that it comes before the actual precinct's transmission. Finally, the central site would immediately identify the problem when it received two transmissions from a precinct (the false one and the actual one).

Computer experts suggest that increasing the security and encryption level of the results transmission is the only way to greatly reduce this risk. Most of these theories fail to consider all of the procedures and verification mechanisms already safeguarding elections. Nevertheless, several additional procedures can be put in place to minimize this potential security vulnerability.

The Secretary of State will incorporate into the Procedures Manual a procedure that clearly defines the election results transmission process and eliminates any risk in this area. This will be accomplished by establishing procedures that:

- Make election officials aware of the potential risk;
- Establish rules regarding securing transmission channels when they are not expected to be in use;

- Create guidelines for handling cases where multiple transmissions are received from one precinct (which could identify a problem);
- The dial-up Point-to-Point Protocol (PPP) authentication currently uses Password Authentication Protocol (PAP). It is recommended that election system vendors use challenge-response authentication protocol (CHAP) when transmitting election results; and
- Mandate a policy that requires a double check of all election results by comparing the precinct paper tape to the transmitted results.

2. Establish contingency plans in the event that outside contractors are unable to perform their duties.

As a result of size and resource constraints, several counties in Arizona outsource election related tasks to local vendors. These tasks include ballot design, election programming services, and ballot printing coordination. Although it is recognized that the counties should be able to outsource election related functions if necessary, the reliance on a single vendor raises concerns in the event that the vendor is unable to perform its duties at a critical time during the election cycle.

The Brewer Plan recommends that all counties develop a contingency plan to assure that critical election tasks will be accomplished. These contingency plans should include, but are not limited to the following:

- Participation in statewide election equipment user groups;
- Continuous training of key employees to perform the more essential election related functions currently being outsourced;
- The sharing of knowledge and resources between neighboring counties; and
- Ongoing renewal of maintenance and support contracts with election equipment vendors.

The Secretary of State's Office will continue to work with the counties to solidify their contingency plans for the 2006 Federal Elections.

3. Establish minimum standards of emergency preparedness for all counties.

The increased awareness of homeland security has affected the election process. It is necessary for election officials to have a complete contingency plan in place in case of an emergency. In developing this contingency plan, it is necessary to balance polling place security with the need for voter accessibility.

There is always the possibility of an unforeseen event disrupting the election process. For example, Arizona polling sites have been moved because of bad weather, toxic spills, and bomb threats. Fortunately, these events have always been handled without seriously disrupting any election. It is

necessary, however, to ensure that our county election officials are prepared to deal with an unforeseen event that may arise during an election.

All counties have some level of emergency plans in place. The Secretary of State's Office has determined that the level of preparedness in planning for unforeseen events varies among the counties. In addition, homeland security has expanded the types of contingencies for which planning needs to occur. The Secretary of State will collaborate with the counties to review current plans and homeland security guidelines, develop revised minimum standard of emergency preparedness, and implement the revised emergency preparedness plans prior to the 2006 Federal Elections.

4. Strengthen laws, policies, and procedures concerning recounts and contested elections.

An automatic recount occurs if the margin between two candidates or votes cast for and against a ballot measure fall within a small margin set by statute. In addition, any elector can file a contest action within five days after the election is canvassed. A recount and contest proceeding may be combined into one court proceeding. The statutes establishing recount and contest procedures have been in existence for decades. It is now time to revisit these statutes in light of the election process and technology currently in use today.

There are certain known changes that will help improve these laws, policies and procedures. For example, this past election revealed a discrepancy between the procedures and Arizona Statutes regarding ballot storage. Legislation will be sought in 2005 to fix that problem and the Procedures Manual will be revised accordingly.

Other issues surrounding recounts and contested elections need a comprehensive review. Changes should be proposed if the review reveals any flaws or shortcomings in the current laws, policies, or procedures including appropriate auditing processes. The topic of manual recounts was raised during the 2000 and 2004 elections. Because of questions surrounding the accuracy of manual audits and recounts, there are concerns as to whether this is the right solution for Arizona. Studies are currently being conducted to measure the accuracy of different counting methods, including manual counts. NIST and the EAC are also studying manual recounts and the reliability of vote tabulation equipment. A committee appointed by the Secretary of State will perform a comprehensive review by evaluating the recent studies, best practices, and other relevant material related to recounts and contested elections. The committee will be asked to issue a report to the Secretary of State prior to December 31, 2005.

5. Clarify and enhance polling place procedures regarding physical set up, poll workers, and observers.

To assure uniformity throughout the state, it is recommended that the procedures followed in each polling place on Election Day be in compliance with the guidelines outlined in the Secretary of State's Procedures Manual. Polling locations vary a great deal, but uniformity in the basic set up and operation of the polling place will help to ensure a more efficient system for voters on Election Day.

Proper protocol for poll workers and party observers is one area that will be addressed. It is also recommended that all counties offer Premium Election Board Worker Training. This is voluntary training that is more intensive and covers more material than the statutory pre-election training currently required of poll workers. This training is provided for in statute and is currently offered in several counties. Attendees are tested at the end of an eight-hour training, and receive “certified” status. Those who do not get a passing score will have an opportunity to attend future classes, or study the handbook and re-take the test. The Secretary of State will work with county election officials to establish guidelines and curriculum for these trainings.

6. Improve logic and accuracy testing procedures.

Logic and accuracy tests are performed before every election to ascertain that the equipment and programs will correctly count the votes cast for all offices and on all measures as required by A.R.S. § 16-449. A post-election logic and accuracy test is performed after the official count has been completed but before the canvass. The software and data used to set up the election, tabulate the ballots and conduct the pre-election logic and accuracy test for each election is used to conduct the post-election logic and accuracy test. The equipment used to conduct the initial logic and accuracy test shall be used to demonstrate that the software and data used to perform the pre-election logic and accuracy test and tabulate the ballots is the same software and that no changes have occurred.

These tests demonstrate that:

- each candidate and ballot measure receives the proper predetermined number of votes,
- the system reports the proper number of overvotes, as required by A.R.S. § 16-449, and
- the system accepts only the proper ballot styles and rejects improper ones.

The logic and accuracy test is conducted by processing a preaudited group of logic and accuracy test ballots marked to record a predetermined number of valid votes for each candidate and on each measure. The test also ensures that for each office one or more ballots have votes in excess of the number allowed by law in order to test the ability of the automatic tabulating equipment and programs to reject overvotes. The methods for uploading the results into the accumulation program is also tested. The accuracy certification board compares the results from the test to the predetermined results.

The logic and accuracy test is observed by the accuracy certification board, consisting of two members who are not from the same political party, and is open to the public and media.

Improvements and changes should be made to the logic and accuracy testing procedures due to the introduction of new voting equipment along with the effort to improve the quality of the election process. Areas to improve the process include:

- Implementing a new policy on the optimal timeframe between the logic and accuracy test and the actual election. Ideally, the logic and accuracy test should occur as close to the Election Day as possible. The increased amount of voting equipment and the geography of the state make it necessary for election officials to have enough time to thoroughly perform

the test. The revised process will evaluate the optimal timeframe for performing the logic and accuracy test.

- Testing election equipment for logic and accuracy in election mode. The election equipment has the option to be logic and accuracy tested in either test mode or election mode. The Secretary of State's Office performs a logic and accuracy test in each county prior to every election. The Secretary of State's Office will perform the logic and accuracy test in election mode. Testing the machines in election mode is a more accurate method for testing the equipment.
- The best way to logic and accuracy test touch screen voting systems. New procedures will be drafted on how to logic and accuracy test touch screen voting systems in an efficient and accurate manner.

II. INCREASE VOTING SYSTEM SECURITY PROCEDURES TO RAISE PUBLIC CONFIDENCE IN ELECTIONS.

It is the role of election officials to protect and promote public trust and confidence in the election process. The foundation of our democracy is the fundamental faith that our citizens have in the fairness of our elections. The success of the democratic process depends upon fair, open, and secure elections, which accurately reflect the intent of the citizens.

Providing secure elections plays a critical role in garnering public confidence in the election process. Secure elections include maintaining the physical security of the equipment and supplies and also protecting electronic equipment from unauthorized access or computer attacks.

Election security is of utmost concern to Secretary Brewer. In addition to the recommendations below, as a member of the EAC Standards Board, Secretary Brewer will continue to work and advocate for stricter federal standards for election security.

This section of the Brewer Plan identifies several steps that should be taken to ensure that Arizona's elections continue to be conducted in a fair, open and secure manner.

1. Implement minimum statewide standards and procedures for physical storage and transport of election machines and ballots.

Arizona counties vary in size, resources, and facilities and have their own procedures for physical security when it comes to elections. These include security surrounding the storage of voting machines and ballots, and the manner in which machines and ballots are transported to and from the polling locations.

The Secretary of State along with county election officials will set minimum statewide standards and procedures for physical storage and transport of election machines and ballots. These changes will be set forth in the Procedures Manual.

2. Seek legislation to increase penalties for tampering with election equipment or software.

The Secretary of State will seek legislation to make it a Class 5 felony to tamper with any component including software, source code, or hardware used for elections. Election officials will be asked to post a notice regarding the penalties for tampering with any component of the voting system in the polling locations.

3. Implement minimum polling place security procedures to ensure no malicious tampering occurs with election equipment or software.

Election security demands that sound procedures be put in place and followed without variance. Comprehensive and consistent security procedures at the polling place will help ensure that no malicious activity can occur with voting equipment and instill public confidence in the process.

The Secretary of State along with county election officials will set minimum polling place security procedures. All counties should be required to develop a physical security plan regarding all of the components of the voting system, including the details of how the chain of custody of each component is monitored and documented.

4. Implement procedures to ensure that proper security methods and practices are applied to all election system software and hardware.

All election tabulation machines depend on hardware and software to operate. Although every county has some level of computer security in place, the level of security and practices varies.

The State of Arizona should adopt computer security procedures to assure that all counties follow uniform standards regarding election system software and hardware. The procedures should cover topics such as:

- User ID and password maintenance;
- Security patches;
- Standards for transmitting election results;
- Turning unneeded services off;
- Bios security and lockdown procedures;
- Authorized access to voting equipment; and
- Proper auditing.

5. Implement procedures to ensure that election systems are not connected to the Internet and that election equipment is used only for election purposes.

The election systems used in Arizona should not be connected to the Internet in any manner. It is acceptable for election equipment to be networked separately, but that network cannot be connected to any other network or the Internet. This will eliminate any possibility of an Internet attack.

Some election equipment uses standard computer hardware and software. It is possible for this equipment to be used for other office related tasks unrelated to the election. New procedures will require that election hardware and software be used only for election purposes.

III. REQUIRE A VOTER VERIFIABLE PAPER BALLOT OR RECORD FOR ALL TYPES OF VOTING SYSTEMS USED IN ARIZONA.

Many state and local jurisdictions have moved towards direct record electronic (DRE) voting systems. This technology allows a voter to cast a ballot using a touch screen. The vote is tabulated electronically and no paper ballot or record is generated. These states and jurisdictions have faced a flurry of criticism and lawsuits by many individuals and groups that believe this technology is insecure and vulnerable to memory and equipment failures, software corruption, and electrical component flaws.

With so many unknowns in the future for touch screen systems, Secretary Brewer urged a cautious approach when choosing which equipment to replace the antiquated punch card voting machines still being used in Arizona prior to 2004. Instead of choosing to purchase touch screen voting machines, the decision was made to replace the punch card machines with proven optical scan voting technology. Another factor entering into this discussion are the opposing demands of the groups that want paper ballots for all voting systems and the disability community that prefers voting systems that enable independent and private voting on electronic voting devices that may not produce a paper ballot or record. HAVA calls for voting system to be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters. The ultimate solution for the elections in 2006 must balance the needs of both communities to the best extent possible.

The Gartner study concluded that DRE or touch screen technology may be used safely and effectively and does not require the use of a paper ballot, but the ongoing nationwide controversies over this technology could ultimately force changes to existing federal standards. Although these claims have yet to be substantiated and virtually every legal challenge brought against this technology to date has failed, public confidence is clearly below what it should be.

Based on this review, new developments in technology, and experience gained from an experimental pilot project conducted during the 2004 General Election, Secretary Brewer has concluded that any voting system used in Arizona must have a voter verifiable paper record or ballot that visually indicates all votes cast.

1. Optical Scan technology will remain the primary tabulation technology used in Arizona.

As stated previously, HAVA mandated the replacement of punch card voting machines and also requires that at least one DRE voting system or other voting system equipped for individuals with disabilities be placed at each polling site by the 2006 Primary and General Elections. Through the "Adios Chad" program administered by Secretary Brewer in 2003, all counties in Arizona now utilize optical scan technology as their main election system. Optical scan technology provides a voter verifiable paper ballot that visually indicates all votes cast. The optical scan paper ballots are machine-readable so that, in the event of a recount, they may be quickly and accurately processed.

Optical scan technology is the optimal technology at this time because:

- It relies on a paper ballot that indicates clearly the selections made by the voter and is machine-readable;
- It is flexible enough to accommodate both onsite voting in the polling place and early or mail voting;
- In the unlikely event of an equipment failure, the ballots are always available for subsequent review and inspection; and
- It is the optimal technology to handle additional voter volumes at the polling locations. Each polling location only needs one optical scanning machine, but can set up many voting booths. No additional electronic equipment is needed to set up additional voting stations.

Consequently, it is recommended that optical scan technology continue to be the primary voting tabulation technology used in Arizona.

2. Any accessible voting device (DRE or touch screen voting machine) will be required to have a paper ballot or record that visually indicates all votes cast.

In 2003, the primary direct recording electronic (DRE) technology was touch screen machines that tabulated votes, but did not provide any paper record to the voter indicating what the voter selected. The voter could only review his or her votes on the touch screen before casting the ballot. At that time, touch screen technologies that provide a paper record to the voter had not gone through an independent testing authority (ITA) certification as required by Arizona law.

The Secretary of State will issue a Request for Proposal (RFP) in 2005, inviting vendors to bid on the contract to place an accessible voting device in each of Arizona's 2,000 plus polling sites prior to the 2006 Federal Elections. Initially, the intent was to purchase the original touch screen system that did not produce any type of paper record or ballot. After observing the issues raised in other jurisdictions using these devices in 2003 and 2004, Secretary Brewer chose to delay the purchase of these systems until the issues surrounding this technology could be studied further.

Because of diminished public confidence in DRE or touch screen voting devices that do not produce a paper record, the RFP issued by the Secretary of State will require that each accessible voting device produce a voter verifiable paper record or paper ballot that visually indicates all votes cast. Vendor selection is expected by mid-year 2005. All polling locations in Arizona will have a new accessible voting system that will allow individuals with disabilities to vote in a manner that provides the same opportunity for access and participation as for other voters. The voting systems will produce a paper ballot or record before the first federal election in 2006.

One such technology came to the attention of Secretary Brewer early in 2004 and through her efforts Arizona became the first state in the country to participate in a pilot demonstration project of this technology at the November 2, 2004 General Election. This technology provides an accessible touch screen voting environment to disabled voters while also producing a standard paper ballot that can be read by existing optical scan equipment.

This pilot project was broken into two different phases. The first phase included various hands-on demonstrations of the new technology during the summer and fall with members of the disabled community, minority groups, and literacy groups. There was significant interest, attendance, participation, and interaction with the new technology. The second phase involved a limited experimental use of this equipment as part of the November 2, 2004 General Election. This experimental use during the election was limited to Maricopa, Cochise and Graham counties in six different precincts.

Voters were given the opportunity to vote on the machines, which marked official ballots. Sixty-five voters cast their ballots using the system and filled out surveys that will be reviewed by the Secretary of State's Office as it determines how best to meet the HAVA 2006 accessibility requirement. The overall response was very favorable with most participants indicating they would willingly use this technology again in a future election.

While it is not known whether this specific technology will be chosen as the final solution for Arizona's accessible voting needs in 2006, it serves as one example of the type of technology that may satisfy the requirements of this recommendation.

All vendors will be required to competitively bid through the state procurement process for providing accessible voting systems to Arizona. The procurement process will allow Arizona to see what the state of technology is with touch screen voting devices along with helping to determine which technology will meet the new requirement of a paper record or ballot that is verifiable by the voter.

IV. INCREASE THE SHARING OF INFORMATION AND LESSONS LEARNED.

Each of Arizona's 15 counties is primarily responsible for administering the federal and state elections. These responsibilities are shared by the county board of supervisors and the county recorders and include preparing, printing and providing sufficient ballots, mailing sample and early ballots to voters, training poll workers, tabulating and storing ballots. The Procedures Manual sets forth rules that have the force of law and are followed by the counties in administering these responsibilities in a correct, impartial, uniform, and efficient manner. Nevertheless, it is impossible for the Procedures Manual to cover every possible administrative task and function performed by the counties. Thus, it is important for regular communications to occur to ensure the greatest degree of uniformity possible. This section sets forth recommendations to accomplish this objective.

1. Establish semi-annual post election meetings of county and local election officials to identify and recommend voting system procedure improvements.

In order to maximize the potential for conducting fair and accurate elections, it is vital that all counties follow uniform guidelines. The Procedures Manual is one of the tools used in working toward the goal of uniformity. The implementation of new voting equipment in Arizona has resulted in the need for new procedures for the conduct of elections.

The Election Officials of Arizona currently hold post election meetings in April and November each year to discuss lessons learned in the election process. Discussion points for these meetings include not only uniform organizational approaches to election management, but also proposed legislation and changes to the Procedures Manual. It is recommended that election officials seek out public comment, poll worker input, and poll worker evaluations for further topics of discussion at these meetings to ensure that the end goal of improving the election process in Arizona is achieved.

2. Increase the sharing of information among election officials using similar equipment by establishing user groups.

Nine of Arizona's 15 counties first began using optical scan voting equipment during the Presidential Preference Election held on February 3, 2004. These counties all put into use the Diebold AccuVote optical scan machine purchased through the Secretary of State's "Adios Chad" program in 2003. The remaining six counties have been using similar optical scan technology since as early as 1996. Of these six counties, three use equipment manufactured by ES&S and three use Diebold equipment. The experiences of these six counties have proven invaluable as the nine counties transition to the new voting technology.

During the transition, the Secretary of State felt it would be advantageous to form user groups. The information and experiences shared within these groups has played an integral part in the success of the "Adios Chad" implementation.

Both ES&S and Diebold have been willing participants in the user group meetings. Many of the concerns and apprehension expressed by the counties have been addressed as a result of the vendor's presence. These meetings should continue semi-annually or be held more frequently if the need arises.

3. Implement a communication schedule with Arizona vendors of election systems to ensure compliance with Arizona policies and procedures.

As proven with vendor attendance at the Diebold User Group meetings, communication between the state, counties, and the election equipment vendors is of the utmost importance. The Secretary of State will meet with existing vendors of both election equipment and voter registration systems on an annual basis to cover changes in technology and legislation that will affect the voting process and to ensure that the vendors are complying with Arizona's election laws and procedures.

4. Conduct public meetings to discuss election topics.

One of the largest contributing factors to the public's confidence in elections is their understanding of the process. Election officials are encouraged to hold public meetings prior to elections to assist in public understanding of election processes and procedures.

V. PROVIDE FORMAL SECURITY AWARENESS INFORMATION, TRAINING, EDUCATION, AND PROCEDURES.

Elections are complex events and require a substantial amount of work to administer successfully. The changes to election technology and Arizona's tremendous population growth add to the complexity of planning and executing an election. The keys to success are properly trained election officials, properly trained poll workers, and an electorate that understands the voting process. This section of the Brewer Plan sets forth recommendations to provide formal security awareness information, training, and education.

1. Enhance election official training by expanding election curriculum and offering training to all county and local election personnel.

Proper training is a key component to ensure that election officials are properly equipped to perform their responsibilities. Election official certification training includes such items as education on new laws, election policies and procedures, real election situations, and hands on experience of voting system equipment.

It is recommended that election official certification training be made available to city election officials to help ensure uniform and secure elections statewide.

2. Enhance poll worker training guidelines.

Poll workers are often the first and only personal contact that citizens have with the election process and are the backbone of any successful election. Several thousand individuals worked the polls during the 2004 Primary and General Elections. These individuals often work 16 or more hours on Election Day with few breaks. It is imperative that qualified people be recruited to work the polls and that these individuals be properly trained to assure that the elections are conducted in a secure, fair and uniform manner.

On Election Day, poll workers welcome voters, facilitate voting, conduct precinct operations in accordance with election law, instruct voters, and follow carefully defined procedures. Poll workers are a large part of the goal of providing a satisfactory Election Day experience for all voters.

Poll workers attend mandatory training sessions to prepare them for their responsibilities. The Procedures Manual provides general guidance to the counties on topics to be covered during the training. The counties, however, are responsible for performing poll worker training, and the quality and level of training can differ from county to county.

It is recommended that the Secretary of State's Office enhance existing guidelines regarding the minimum standards for all counties to follow when performing poll worker training to ensure statewide uniformity and an increased emphasis on security.

3. Provide state funding for poll worker training.

Poll workers only work during the four election periods each year. Election officials have challenges recruiting, retaining, and training poll workers. The Secretary of State's Office will provide funding to counties to establish more comprehensive poll worker training curriculum, obtain better training materials, enhanced "Premium Board Worker" training, and assist in delivering proper poll worker training. The funding cannot be used for poll worker compensation, as that is the counties' responsibility.

4. Increase state funding for voter outreach to ensure the public is informed about election systems and procedures.

The primary purpose of voter outreach is to reach those populations who traditionally have been under-represented at the polls or who are not informed about the registration and voting process. Past elections have demonstrated that many voters misunderstand the election process. For example, it was learned during the 2004 elections that voters who use the wrong type of writing instrument on their early ballot may not have all of their votes counted accurately. Other potential voters did not register to vote in time to participate in the 2004 elections because they did not understand the registration process. Additional voter education is a critical component to increasing voter participation.

The Secretary of State's Office and the counties take voter outreach seriously. The Secretary of State's Office purchased advertising statewide to educate voters about the new equipment, published material in both English and Spanish, and performed nearly 40 town hall meetings prior to the 2004 General Election even though only three were required by law. The counties also engage in extensive voter outreach, including substantial programs that target Spanish speaking and Native American voters.

The Help America Vote Act, Proposition 200, new voting equipment, and other changes in state law all add to the need for the public to be well informed on election matters. Some of the changes in state and federal law have the potential to increase the number of provisional ballots cast along with adding steps at the polling location. Election officials have a very difficult task when running elections. Election laws are consistently changing; voter turnout is unknown until the day of the election; finding qualified poll workers who can give up an entire day; and other factors make it difficult to run a trouble-free election. Arizona election officials did an outstanding job in 2004 considering the large voter turnout for the 2004 Presidential Election. Long lines at certain polling locations in 2004 caused some citizens to complain. Without taking proactive steps, future elections could encounter problems with long lines and voter confusion.

One of the most effective ways to reduce problems on election day is to have a well informed voting population that understand the voting process. Voter education has a direct and proportional effect on the number of provisional ballots cast. If citizens maintain their voter registration records, election officials can plan properly and ensure that each of the polling locations have the proper amount of voting equipment and poll workers. If citizens know how to find their polling location, voter confusion is further reduced.

It is recommended that the Secretary of State's Office increase funding for voter outreach efforts to continue to make sure voters know how to properly register to vote, educate the electorate on the voting process from start to finish, and instruct the voter on how to obtain needed information. Voter outreach should also aggressively reach out to underserved groups to include them in our democratic process.

VI. STRENGTHEN CURRENT STATE CERTIFICATION POLICIES AND STANDARDS FOR VOTING EQUIPMENT AND SOFTWARE TO INCREASE VERIFIABILITY AND TRANSPARENCY IN THE ELECTION PROCESS.

In addition to Federal Voting System Standards established in 1990 and revised in accordance with HAVA, Arizona law requires state certification of all voting equipment. Under Arizona law, the Secretary of State is responsible for certifying voting equipment and for establishing practices to run elections, tally results, and handle ballots.

In accordance with Arizona law, the Secretary of State appoints a three-member committee to review election equipment and make recommendations to the Secretary of State regarding approval for use in state and local elections. Although the law requires the panel to test the various machines, it does not prescribe the manner in which the machines shall be tested.

The certification of voting equipment in Arizona continues to evolve and Secretary Brewer has made substantial enhancements to the certification process. This section identifies additional measures that should be taken to improve the certification process.

1. Require software and firmware source code be held in escrow.

Though it has historically been a condition of certification, in 2003 Secretary Brewer successfully advocated for legislation requiring all voting equipment presented for Arizona certification to first receive full testing and certification by a laboratory accredited in accordance with HAVA. All testing laboratories authorized by the EAC have access to the source code of election system commercial software developers and that code is thoroughly reviewed prior to certification.

There are those who believe open source code review of election system software and firmware should be required. Open source generally implies that the code is available for review by anyone, anywhere and that it is typically published on the Internet for such availability. This level of exposure would permit competitors to ascertain exact methods and techniques of their competition, thus rendering superior application development no longer a competitive edge. More importantly, it would make it possible for anyone who understands the system's vulnerabilities to subvert the system, there would seem to be little public good gained from such exposure.

It is therefore recommended that vendors must place all application source codes into either public domain or software escrow, and authorize the state as the recipient of escrow before a voting system may be used in a state election. This action would allow qualified state staff to review such source codes if and when it became necessary while also protecting the vendor's right to keep that code private. The requirement also includes the vendor placing the software executable and software compiler in escrow. The compiler is necessary to ensure that the source code can be converted into an executable software program that can be run on a computer. The Secretary of State will require in its contracts with vendors that all voting system software and firmware source code be subject to review by experts at the Secretary of State's discretion.

2. Require all changes to voting systems used in Arizona be certified by the Secretary of State and a national independent testing authorities for full functional and security testing.

There has been voting equipment certification in Arizona since 1985. In the past, modifications made by vendors to previously certified election equipment resulting in version number changes have not received any type of scrutiny. In her ongoing effort to increase the security of Arizona's election systems, Secretary Brewer began requiring that all modifications made to voting equipment undergo qualification by the national independent testing authorities and certification by the Secretary of State's Office before use in an Arizona election. Prior to this requirement, it was unclear when a piece of equipment or software needed to be certified. The new requirement removes all uncertainty regarding when a piece of equipment or software needs to be certified because any change now requires approval by the committee.

3. Implement certification best practices learned from other states and the Election Assistance Commission.

It is recommended that the Secretary of State's Office adopt a best practice certification and de-certification process based upon the recommendations contained in the Gartner study. This process should include a review and recommendation by the three-member certification committee. In addition, it should take into account standards established by the EAC, the unique requirements of voting equipment set forth in Arizona law, and utilize, when possible, the best practices in such states as California and Louisiana. These processes will also include provisional approvals, emergency conditional certification, and system upgrades.

4. Ensure that only certified software, hardware, and firmware are used in Arizona elections.

In order to ensure that only certified software, hardware, and firmware are used in Arizona elections, it is recommended that a written communication be sent to all Arizona election system vendors informing them of the new certification procedures that include configuration management. Counties, cities and local jurisdictions should also receive additional training about certification requirements during the biennial election official certification training conducted by the Secretary of State. The responsibility of assuring that all voting equipment in use is certified falls upon the vendor and respective county or local jurisdiction. The affected jurisdiction should take steps to verify the certification status of its voting hardware, software, and firmware, and any modifications to such prior to its use.

5. Post all certified election equipment and software on the Secretary of State Web site.

Beginning January 1, 2005 all certified and decertified equipment, firmware, and software in Arizona will be posted on the Secretary of State Web site. This will allow the public to have full access to that information.

6. Seek legislation to allow the Secretary of State to grant conditional emergency certification when warranted.

Secretary Brewer has demonstrated her commitment to the voting equipment certification process by expanding its application as discussed above. All equipment and software modifications and upgrades must now be approved through the certification process prior to use. It is recognized, however, that the national testing process by the ITA's can take up to 12 months. An unforeseen circumstance could arise that would call for the modification of software close to an election and without sufficient time to undergo the ITA qualification process. Therefore, it is recommended that legislation be adopted to enable strict new processes and procedures for emergency certification.

Emergency certification should only occur when other options have been exhausted or determined not to be feasible and the county election official has taken the emergency certification request to the local governing board such as the County Board of Supervisors for their approval in an open meeting. Emergency certification can only occur on equipment or software that has had a version certified before; no new hardware or software can qualify. The emergency certification should only last for six months.

The emergency certification process should be rare and only used when absolutely necessary. In addition to approved election equipment and software, beginning January 1, 2006, the Secretary of State will post on its Web site any equipment or software that has been approved for use with an emergency certification and the duration of that emergency certification.

7. Require county election officials to certify once every election that only certified hardware, firmware, and software is in use.

This recommendation adds an additional check to ensure that only certified hardware, firmware, and software is being used in Arizona.

VII. IMPLEMENT STANDARDS AND RECOMMENDATIONS FROM THE ELECTION ASSISTANCE COMMISSION (EAC).

The Election Assistance Commission (EAC) was created by HAVA. The EAC was established to assist in the administration of federal elections and to otherwise provide assistance with the administration of certain federal election laws and programs, to establish minimum election administration standards for states and units of local government with responsibility for the administration of federal elections, and for other purposes. Within the scope of this task are voting systems, voter registration, administration of payments and grants, and research. The work of the EAC will continue indefinitely and should be continuously followed by our state and local election officials in accordance with the following recommendations.

1. Review and evaluate all recommendations and best practices set forth by the EAC.

As Arizona's Chief Election Official, Secretary Brewer is a member of the EAC Standards Board composed of 110 members drawn from State and local election officials. The Standards Board (acting through its Executive Board) and the Board of Advisors review proposed voluntary voting system guidelines and EAC technical guidance.

Various tools will be used to accomplish the monumental goal of this Commission. One already in place is the Post General Survey that requires each state to report such statistics as ballots cast, early ballots requested, equipment failure and handicap accessibility at the polling places. The state is responsible for collecting and correlating information for this survey that will provide a benchmark for future development of guidelines and standards for elections and election equipment.

It is recommended that the Secretary of State's Office continue to review and evaluate all recommendations and best practices set forth by the EAC. These recommendations should be incorporated into the Procedures Manual when appropriate.

VIII. MODERNIZE ELECTION EQUIPMENT AND SOFTWARE.

As discussed in Section III, it is recommended that optical scan technology continue to be the primary technology used to conduct Arizona's elections and that the accessible voting devices purchased to comply with the 2006 HAVA mandate produce a voter verifiable paper record or paper ballot that visually indicates all votes cast. As we move forward it is also recommended that Arizona's current election equipment and software continue to be studied and monitored to assure that Arizona's election systems are operating in the best possible manner.

1. Replace antiquated punch card voting machines with optical scan technology.

In 2003, the Secretary of State distributed over three million dollars to replace punch card voting equipment still in use in nine counties with new optical scan vote tabulation systems and election management systems. Additionally, Cochise County qualified for federal reimbursement for their recently purchased optical scan system.

Beginning with the 2004 Presidential Preference Election, all 15 Arizona counties successfully used optical scan voting systems. There are now only two election system vendors operating in Arizona. Twelve of the 15 counties use Diebold voting equipment and three counties use Election System and Software (ES&S) voting equipment.

The replacement of punch card voting technology with optical scan technology was a major step taken by Arizona to modernize its voting equipment and software.

2. Provide accessible voting devices for voters with disabilities.

The Secretary of State will distribute millions of dollars to Arizona counties in 2005 to purchase accessible voting systems in time for use in the 2006 Federal Elections. Arizona will purchase one accessible voting system for each of the 2000 plus precincts as well as a defined percentage of spares. The purchase of these voting systems will further contribute to the modernization of Arizona's voting equipment and software.

3. Continue to monitor the state of the election equipment industry.

The Secretary of State takes an active role in defining future standards of election equipment by participating on the EAC Standards Board. She will work in this capacity to impose additional federal standards on equipment vendors to improve security, accessibility, and voter confidence.

Several organizations, committees, and boards exist within the election community. The Secretary of State maintains close ties with the Election Assistance Commission, National Institute for Standards in Technology, National Association of Secretaries of State, and the National Association of State Election Directors. She will continue to be updated on industry developments through her contacts with these organizations.

Because the Secretary of State must certify all election equipment before it can be used, she is in an excellent position to maintain close contact with the vendors doing business in Arizona. The Secretary of State will work with election equipment vendors to monitor trends in election equipment and ensure that vendor equipment meets Arizona's strict certification requirements.

The Secretary of State continues to urge a cautious approach when it comes to implementing new technologies to assure that the technology is proven, secure, and reliable.

4. Develop a statewide election equipment refresh policy.

Election equipment is a major capital expense for Arizona's counties. As with any technical equipment, election equipment eventually wears down, becomes antiquated, may cause problems, and requires replacement.

A standard equipment refresh policy ensures that all counties have adequate systems to effectively run accurate elections. It also provides the criteria necessary for counties to properly plan for the expense of equipment replacement. Therefore, it is recommended that the Procedures Manual include a policy that defines a statewide election equipment refresh standard.

IX. ENHANCE THE STATEWIDE VOTER REGISTRATION SYSTEM.

A voter registration system is intended to protect the integrity of the electoral process by ensuring the maintenance of an accurate and current voter registration list. A quality voter registration system will remove ineligible voters and minimize the problem of individuals registering to vote in multiple jurisdictions, whether intentional, through fraud or unintentional, through relocation and failure to cancel a previous registration. Having a properly functioning voter registration system is necessary to increase confidence in the electoral process.

This section of the Brewer Plan identifies several steps that should be taken to improve the quality of the voter registration processes and data in Arizona.

1. Enhance the statewide voter registration system with improved processes and technology to ensure accurate voter registration rolls.

The State of Arizona implemented the Voter Registration Arizona (VRZA) system on January 1, 2004, as mandated by HAVA. Although the majority of states chose to wait until 2006 to implement their statewide voter registration system, Arizona insisted on pushing forward. The program was created to help improve the voting process in Arizona by increasing voter registration and improving the quality of the voter registration roll.

Arizona is one of the fastest growing states in the nation and is culturally and geographically diverse. The state has 15 counties that prior to VRZA were each responsible for maintaining separate voter registration rolls. There was no effective mechanism in place to ensure that someone was not registered in multiple counties. The checks to determine if someone had died or was prohibited to vote due to a felony conviction were not performed centrally and methods to do so varied among counties.

VRZA addresses these issues to ensure the accuracy, integrity, and uniqueness of the statewide voter registration list by reducing the amount of duplicate registrations and cleaning the voter registration rolls. This is accomplished by comparing voter registration records on a statewide basis against death, felony, and motor vehicle records. The VRZA system performs statewide comparisons in four major areas:

- **Motor Vehicle Records** - All new additions to the voter registration database are matched against the Arizona Motor Vehicle Division (MVD) database. Any changes to a voter's identifying information in the voter registration system are compared to the driver license or non-operating identification license database. The voter registration form requires either a driver license/non-operating identification license number or the last four digits of social security number be entered. The voter registrant's name, date of birth, driver license/non-operating identification license number or last four digits of social security number are compared against the Motor Vehicle Division database. All driver licenses or non-operating identification licenses in Arizona require a valid social security number that is verified against the Social Security Administration database. Each day, the VRAZ system notifies the counties of the results of the MVD matching.
- **Duplicate Matching Across Counties** - All new additions to the voter registration database or any voter that moves from one county to another has their record compared with all records in other counties to determine if it is a duplicate record or not. Each day, the statewide voter registration system notifies the counties of the results of the duplicate matching.
- **Court Record Matching** - The Secretary of State's Office sought legislation in 2003 to allow all court records to be matched with voter registration records at the state level. Since the legislation passed, all court records for felony and incapacitated cases from the United States District Court and the Arizona Superior Court received by the Secretary of State's Office are compared to the entire voter registration database. The statewide voter registration system notifies the counties daily of the results of the court record matching.
- **Death Record Matching** - The Secretary of State's Office sought legislation in 2003 to allow all death records to be matched with voter registration records at the state level. Since the legislation passed, all death notification records from the Arizona Department of Health Services are received by the Secretary of State's Office and then compared to the entire voter registration database. The statewide voter registration system notifies the counties of the results of the death notification matching.

The State of Arizona is in the process of building an improved statewide voter registration database by implementing Voter Registration Arizona II (VRAZ-II). The new statewide voter registration system (VRAZ-II) will more tightly integrate and automate the processes and relieve the counties of some of the current data entry. Any voter registration record added or updated at the county level will update the statewide voter registration database in real time. In addition, all counties will have updated software and hardware to improve the voter registration process.

The Secretary of State, with input from the county recorders, has modified the voter registration form to improve the usability of the form and to incorporate changes due to Proposition 200. The voter registration form is often the first contact that a citizen has with the election process in Arizona. Public comments and suggestions were incorporated into the newest version of the form.

The Secretary of State is also working with the counties to develop uniform and consistent procedures for processing voter registrations. A citizen's voter registration experience will be

consistent from county to county because Arizona will have uniform and consistent procedures including common voter registration software.

2. Enhance the ability of citizens to know the status of their provisional ballot.

Prior to HAVA Arizona provided all voters the ability to vote a provisional ballot if their name did not appear on the signature roster. Like Arizona, HAVA now requires all states to have provisional ballots and for the citizen who votes a provisional ballot to have a cost free way to find out if their ballot was counted. Arizona's counties have procedures in place to notify voters about their provisional ballots, but the methods vary among the counties.

The VRAZ-II system, when fully implemented, will allow citizens to access the status of their provisional ballot the same way in each county. Arizona will provide a toll free number in addition to Internet access for voters to find out if their ballot was counted. VRAZ-II along with improved procedures will ensure that citizens can find out the status of their provisional ballot within 10 working days.

3. Improve the accessibility of all citizens to the voter registration process.

Arizona's voter registration system and procedures should facilitate easy access to the electoral process by its citizens. There are a number of steps that can be taken to increase this accessibility.

- **Increase Voter Outreach** - Voter outreach efforts by the Secretary of State's Office and the County Recorders help promote voter registration, encourage underserved groups to register to vote, and educate all voters on the election process. These efforts should be increased whenever possible.
- **Automate Voter Registration with Driver License Application** - National Voter Registration Act of 1993 (NVRA) requires that individuals be given the opportunity to register to vote (or to change their voter registration address) in elections for federal office when applying for or receiving services or assistance at any office in the state that provides public assistance, including the Motor Vehicle Division. The purpose of the NVRA is to increase the number of eligible citizens who register to vote. Currently, driver license applicants are asked to check a box indicating if they would like to vote. The MVD employee is then supposed to provide the applicant a registration form to fill out. This system has not worked perfectly in the past and has resulted in confusion when registrants have not received a form, not returned their filled out form, or mistakenly assumed that they became registered by simply checking the box.

The Secretary of State has been working with MVD to fully integrate the Arizona driver license application and the voter registration form so that the same form can accomplish both purposes. The information obtained at the MVD office would then be electronically transferred to the Secretary of State's Office through the EZ Voter program discussed below. This will eliminate many manual steps and help reduce voter confusion. The offices should continue to work together to have this completed by January 1, 2006.

- **Expand Online Voter Registration** - The EZ Voter program enables citizens of Arizona to easily register to vote online in either English or Spanish. The citizen simply enters in their unique information to authenticate and provides other voter registration information. The information provided by the citizen is matched instantly with a motor vehicle record. The demographic information from the MVD record along with the digitized signature from the driver license or non-operating identification license are passed in real time to the Secretary of State's Office and become an official voter registration. The EZ Voter Internet application can be accessed either through the Arizona Secretary of State's or Arizona Motor Vehicle Division's Web sites.

EZ Voter can be viewed as a natural extension of NVRA. Approximately 30 percent of the voter registrations processed during the 2004 election cycle were through the EZ Voter program. The EZ Voter program should be promoted as the best way to register to vote with a goal of increasing the total number of registrations through EZ Voter to 50 percent during the 2006 election cycle.

- **Allow Public Access to Status and Polling Place Information** - State and County election officials should evaluate the best alternatives and feasibility for allowing secure public access to their voter registration status and their polling place location.

4. Ensure that the statewide voter registration database is accessible to county voter registration officials.

Arizona citizens are mobile. It is important that county voter registration officials have current and quality information available when determining a citizen's voter registration status. The VRAZ-II statewide voter registration database will have secured access to authorized election officials to view voter registration information statewide.

5. Seek legislation to improve the quality of voter registration drives.

Some voter registration drives compensate individuals based upon how many voter registration forms they obtain. This compensation may be based on the party affiliation of the person registered. Such a compensation scheme is contrary to voluntary spirit of our democratic process. Moreover, it encourages these drives to solicit registration forms from individuals who are not qualified to vote or who have already registered. The county recorder offices were inundated in 2004 with thousands of invalid voter registration forms that consumed precious resources at a critical time in the election cycle.

If compensation paid to the solicitor is based on the party affiliation of the person registered, it provides a disincentive to the solicitor to seek registration forms from all citizens. The Secretary of State's Office has received inquiries from many citizens who attest that they turned in a registration form to a private get-out-the-vote drive but were never registered to vote. It is difficult to determine exactly why this occurred or who may have been responsible but the possible link to compensation for registering voters of a certain party affiliation cannot be overlooked.

To address these issues the Secretary of State will seek legislation to prohibit compensation of voter registration solicitors based on the number of forms received and the party affiliation of the person registered.

APPENDIX

GARTNER ASSESSMENT OF ELECTION SYSTEMS REPORT

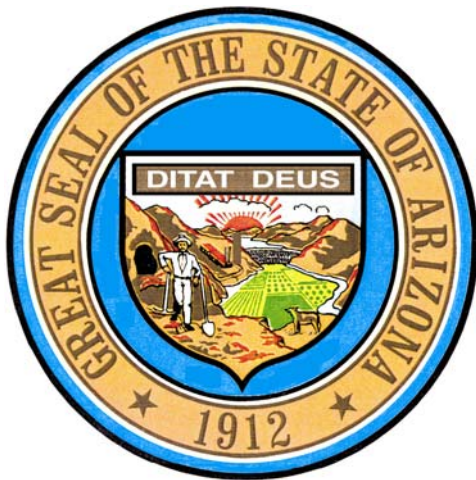


A Report for the

State of Arizona

Assessment of Election Systems

December 2004



Engagement: 220608071

research consulting measurement community news

Gartner

Table of Contents

1.0	EXECUTIVE SUMMARY	4
1.1	BACKGROUND	4
1.2	RECENT ACTIONS BY SECRETARY OF STATE REGARDING VOTING IN ARIZONA	4
1.3	REPORT SCOPE	5
1.4	REPORT OBJECTIVES	5
1.5	REPORT METHODOLOGY	5
1.6	REPORT SUMMARY	6
2.0	QUESTIONS REGARDING THE VOTING INDUSTRY.....	7
2.1	QUESTIONS REGARDING DIRECT RECORD ELECTRONIC (DRE) VOTING EQUIPMENT	7
2.1.1	<i>Can Direct Record Electronic (DRE) Systems Fail and Lose Votes Cast?</i>	7
2.1.2	<i>Is VVPAT Required to Ensure that The Vote Cast Is The Vote Recorded?</i>	9
2.1.3	<i>Are Election System Firms Overcharging to Retrofit for VVPAT?</i>	12
2.2	QUESTIONS REGARDING CERTIFICATION	14
2.2.1	<i>Does the Federal Certification Process Adequately Examine System Security?</i>	14
2.2.2	<i>Do States Need to Conduct Testing Beyond Current Federal Certification Requirements?</i>	16
2.3	IS THE ENFRANCHISEMENT OF THE DISABLED BEING DELAYED?	17
2.3.1	<i>Description</i>	17
2.3.2	<i>Analysis</i>	17
2.3.3	<i>Recommendations</i>	17
2.4	SHOULD ALL SOURCE CODE USED IN ELECTIONS BE “OPEN”?	18
2.4.1	<i>Description</i>	18
2.4.2	<i>Analysis</i>	18
2.4.3	<i>Recommendations</i>	19
3.0	QUESTIONS REGARDING CURRENT DIEBOLD ELECTION SYSTEMS	20
3.1	DO CURRENT DIEBOLD DRE ELECTION PRODUCTS HAVE SECURITY FLAWS?	20
3.1.1	<i>Description</i>	20
3.1.2	<i>Analysis</i>	20
3.1.3	<i>Recommendations</i>	25
3.2	ARE DIEBOLD PRODUCTS VULNERABLE TO INTERNET ATTACKS?	26
3.2.1	<i>Description</i>	26
3.2.2	<i>Analysis</i>	26
3.2.3	<i>Recommendations</i>	27
3.3	DOES DIEBOLD HAVE A QUALITY SOFTWARE DEVELOPMENT METHODOLOGY?	27
3.3.1	<i>Description</i>	27
3.3.2	<i>Analysis</i>	27
3.3.3	<i>Recommendations</i>	28
3.4	DO DIEBOLD PRODUCTS HAVE ADEQUATE CONFIGURATION MANAGEMENT?	28
3.4.1	<i>Description</i>	28
3.4.2	<i>Analysis</i>	28
3.4.3	<i>Recommendations</i>	28
3.5	DO DIEBOLD PRODUCTS HAVE ADEQUATE PASSWORD MANAGEMENT?	29
3.5.1	<i>Description</i>	29
3.5.2	<i>Analysis</i>	29
3.5.3	<i>Recommendations</i>	30
3.6	DO DIEBOLD PRODUCTS HAVE ADEQUATE ACCESS MANAGEMENT?	30
3.6.1	<i>Description</i>	30
3.6.2	<i>Analysis</i>	31

3.6.3	Recommendations	31
3.7	DO DIEBOLD PRODUCTS HAVE ADEQUATE AUTHENTICATION OF ELECTION REPORTING?	31
3.7.1	Description	31
3.7.2	Analysis	32
3.7.3	Recommendations	32
3.8	CAN SMART CARD FRAUD OCCUR WITH DIEBOLD PRODUCTS?	33
3.8.1	Description	33
3.8.2	Analysis	33
3.8.3	Recommendations	34
3.9	DOES DIEBOLD HAVE ADEQUATE INTERNAL SECURITY?	34
3.9.1	Description	34
3.9.2	Analysis	34
3.9.3	Recommendations	34
3.10	DID DIEBOLD DISREGARD STATE-CERTIFIED CONFIGURATIONS?	34
3.10.1	Description	34
3.10.2	Analysis	35
3.10.3	Recommendations	35
3.11	IS DIEBOLD AN OBJECTIVE ELECTION PARTNER?	36
3.11.1	Description	36
3.11.2	Analysis	36
3.11.3	Recommendations	36
3.12	RECENT DIEBOLD ACTIONS IN RESPONSE TO CRITICS	37
3.12.1	Some Perspective	37
3.12.2	In Defense of Diebold Election Systems	37
3.12.3	Response to Ohio Compuware Study	37
3.12.4	Response to the RABA Study	38
3.12.5	Diebold Announces Restructuring of Compliance and Certification Processes	39
3.12.6	Future of Diebold As Election Vendor	40
4.0	QUESTIONS REGARDING VOTING IN ARIZONA.....	41
4.1	HAS ARIZONA ACQUIRED DIEBOLD VOTING SYSTEMS THAT ARE HAVA COMPLIANT?	41
4.1.1	Description	41
4.1.2	Analysis	44
4.1.3	Recommendations	45
4.2	DOES ARIZONA HAVE AN ADEQUATE VOTING CERTIFICATION PROCESS?	45
4.2.1	Description	45
4.2.2	Analysis	48
4.2.3	Recommendations	51
4.3	DOES ARIZONA HAVE SUFFICIENT PROCEDURES TO ENSURE THAT CONFIGURATION CERTIFIED IS CONFIGURATION USED?	51
4.3.1	Description	51
4.3.2	Analysis	51
4.3.3	Recommendations	52
4.4	DOES ARIZONA HAVE ADEQUATE VOTING PHYSICAL SECURITY?	53
4.4.1	Does Arizona Have Adequate Physical Security in Storage of Equipment and Ballots?	53
4.4.2	Does Arizona Have Adequate Physical Security in Transport of Equipment and Ballots?	54
4.4.3	Does Arizona Have Adequate Physical Security at Polling Places?	54
4.5	DOES ARIZONA HAVE ADEQUATE POLL WORKER TRAINING?	54
4.5.1	Description	54
4.5.2	Analysis	55
4.5.3	Recommendations	55

5.0 REVIEW OF SELECTED ARIZONA COUNTY ELECTION SYSTEMS AND PROCESSES56

5.1 DESCRIPTION ----- 56

5.1.1 Apache County----- 58

5.1.2 Pima County----- 61

5.1.3 Yavapai County----- 65

5.1.4 Maricopa County----- 68

5.1.5 Cochise County----- 71

5.1.6 Graham County----- 73

5.2 ANALYSIS AND RECOMMENDATIONS ----- 75

5.2.1 SOS Public Outreach----- 75

5.2.2 SOS County Training, Certification and Qualifications----- 76

5.2.3 Variations of Election Organizations in Counties----- 76

5.2.4 Arizona/Wyoming Ballot Rotation----- 77

5.2.5 Ballot Creation Single Points of Failure ----- 77

5.2.6 Languages ----- 77

5.2.7 “Bug” in Certified Version----- 78

5.2.8 Early Voting----- 78

5.2.9 Election Processing Single Point of Failure ----- 78

5.2.10 Flaw in L&A Testing Method ----- 78

5.2.11 Voter Verifiable Paper Audit Trail (VVPAT) ----- 79

5.2.12 Short Ballot Window ----- 79

5.2.13 Battery on Card----- 79

5.2.14 Retention of Memory Card Data----- 80

5.2.15 Solution for Disability----- 80

5.2.16 Post Election L&A Testing ----- 80

5.2.17 Two-Year Retention Requirement ----- 80

5.2.18 Legal Advice Source----- 81

5.2.19 SLAs Are Lacking in Vendor Contracts----- 81

5.2.20 Continuity Planning and Disaster Recovery ----- 81

1.0 Executive Summary

1.1 Background

Since the Presidential election of 2000, there has been some concern among the people, the states and the federal government regarding the accuracy and reliability of voting systems. In 2002, Congress passed, and the President signed into law, the Help America Vote Act (HAVA), which was intended to address many of the issues surrounding voting and voter registration. In addition, many activists have raised a number of questions in the press regarding voting equipment, most notably with regard to Direct Recording Equipment (DRE), a computer-like technology that displays the ballot and records results on electronic media. Further, much of this discussion has involved the voting systems vendor, Diebold, Inc. (Diebold), in large part because it is the market share leader in the voting equipment industry. Questions have also been raised about voting equipment security, causing some voters to doubt the trustworthiness of systems that do not provide a hardcopy paper trail of the vote cast. This study was commissioned by the Arizona Secretary of State, Jan Brewer, to address these concerns.

1.2 Recent Actions by Secretary of State Regarding Voting in Arizona

The State of Arizona is in an exceptionally good position at this time for the following reasons:

- 1) In 2003, the Secretary of State encouraged the revision of the Arizona law to require (for the first time ever in Arizona) that all voting equipment to be used in Arizona State and local elections must receive full testing and certification by a federally accredited laboratory pursuant to HAVA.
- 2) In 2003, through the Office of the Secretary of State (SOS), Arizona selected optical scan voting technology over the then very popular DRE technology and thus avoided most of the issues that were subsequently raised about DRE voting technology. This was a very prudent decision in light of subsequent events.
- 3) In December 2003, the Secretary of State announced an Action Plan to address statewide voting systems and technology issues. The plan called for new voting system guidelines and increased sharing of information among election offices and annual reviews to enhance election certification policies and standards.
- 4) At the end of 2003, the office of the Secretary of State successfully completed the implementation of a single statewide voter registration system for Arizona (VRAZ), meeting the legislative requirements of HAVA. The system enables accurate and consistent management of voter registration information across all the voting jurisdictions in the state. Arizona was one of only a few states that did not ask for a waiver for the HAVA Statewide Voter Registration List requirement.

In January 2004, The Secretary of State retained Gartner to develop this report as a means by which the SOS can directly take action toward ensuring accuracy and reliability in elections in Arizona.

1.3 Report Scope

There are two fundamental aspects to election systems:

- 1) Voter Registration Systems — Systems that collect, record, verify and track voter registration and voting history.
- 2) Voting Systems — Systems that develop ballots, capture votes cast, tally votes and report them.

This report focuses on voting systems and does not discuss issues regarding voter registration.

1.4 Report Objectives

This report is not an audit. It does not seek to find errors or omissions in the past, but rather is focused on determining best practices “going forward” that will ensure that Arizona elections are fair and accurate and preserve the foundations of democracy.

The objectives of this report are to:

- 1) *Review and Analyze Questions Regarding the Election Industry* — Review questions voiced in news media and in election industry literature regarding the reliability, security and sufficiency of election products and procedures.
- 2) *Review and Analyze Questions Regarding Current Diebold Election Products* — Specifically, review questions related to current Diebold election products.
- 3) *Review and Analyze Questions Regarding Arizona Election Systems and Procedures* — Specifically review questions related to voting system certification, and the security and accuracy of Arizona election systems and procedures.
- 4) *Make Recommendations* — Make recommendations regarding the actions that the State of Arizona should take regarding these issues.

1.5 Report Methodology

Gartner developed this report based upon the following data gathering efforts:

- 1) We reviewed Gartner research on election practices and technologies.
- 2) We reviewed recent reports and articles regarding election technology and security.
- 3) We interviewed members of the staff of the Arizona SOS.
- 4) We visited and interviewed election officials and staff of six Arizona counties. These counties were Maricopa, Yavapai, Cochise, Graham, Apache, and Pima.
- 5) We reviewed progress in other states and focused attention on the certification processes of California and Louisiana as representing best practices in certification.
- 6) We received input from Diebold on the various points concerning their election equipment and systems.

This report was developed section by section with weekly reviews and suggested revisions by SOS staff. This was followed by a comprehensive final review and a public review of the report.

1.6 Report Summary

In keeping with the mission of this report, the main sections of the report focus on the following four (4) question sets:

- 1) *Questions Regarding the Voting Industry* — This section addresses questions that have been raised in the press regarding voting technologies, need for voter verifiable printouts, the certification process, needs of disabled voters and whether the source code of voting systems should be “open.”
- 2) *Questions Regarding Current Diebold Election Systems* — This section addresses questions that have been in the press regarding Diebold election systems.
 - a) This section was concentrated on Diebold for three reasons:
 - i) Arizona has acquired Diebold optical scan voting equipment for deployment in twelve (12) counties to replace their punch card systems.
 - ii) Diebold is the market share leader among voting system vendors.
 - iii) In part because of Diebold’s market position, much of the controversy has been focused on Diebold in the press even though many of the criticisms of them would apply equally well to most other election system vendors.
 - b) Questions in this area review security concerns with Diebold voting equipment, Diebold’s involvement with state certification compliance, questions about Diebold’s objectivity and Diebold’s responses to these criticisms.
- 3) *Questions Regarding Voting in Arizona* — This section addresses questions such as whether Arizona has acquired Diebold voting equipment that is HAVA compliant; whether Arizona has an adequate voting certification process; whether Arizona has adequate voting physical security; and whether Arizona has adequate poll worker training.
- 4) *Review of Selected Arizona County Election Systems and Processes* — This section addresses questions that arose in onsite interviews with the six (6) Arizona counties that were not involved in replacement of their punch card systems with Diebold optical scan equipment in 2003. These six counties were already utilizing optical scan technology for their voting systems.

Though Diebold has been in the news as the center of much of the concern regarding new voting technology and Arizona has purchased voting technology from Diebold, a very fundamental distinction should be made. The controversy is around DRE technology, while Arizona purchased optical scan technology as its mainstay voting technology. This was a very prudent decision on the part of Arizona as many states were acquiring the more attractive DRE technology at that time. Arizona wisely determined that the less high-tech, paper-based optical scan technology was the safer, more reliable and more voter-verifiable technology. This has proven to be true. The Arizona decision-makers in this instance should be recognized for making a wise decision on the selection of voting technology. This decision has enabled Arizona to largely avoid many of the voting systems issues that have been in the news and that are discussed in this report regarding (Diebold) DRE technology.

2.0 Questions Regarding the Voting Industry

2.1 Questions Regarding Direct Record Electronic (DRE) Voting Equipment

2.1.1 Can Direct Record Electronic (DRE) Systems Fail and Lose Votes Cast?

2.1.1.1 *Description*

There is a question as to whether Direct Record Electronic (DRE) systems are vulnerable to failure, as are other computer equipment, due to causes such as hardware memory failures, disc “crashes,” software corruption and electrical component flaws. These failures could be caused intentionally or unintentionally, resulting in the loss of recorded votes with no “artifact” such as a paper ballot remaining that would enable an accurate recount of votes.

2.1.1.2 *Analysis*

All electronic equipment is prone to failure due to a wide variety of causes, and DRE voting systems are electronic equipment. There are five key causes of DRE system failure:

2.1.1.2.1 *Power Failures*

The equipment can be damaged or rendered unusable due to absence of electrical power, or power surges or sags that result in data corruption and inaccurate vote recording or tallying. Simple punch card systems are not electronic and therefore are immune to power conditions¹. Electro-mechanical lever machine voting systems depend on power, but are not electronic and therefore are not as sensitive to power failures or fluctuations. Systems that use electronic components² are sensitive to power fluctuations and can easily be damaged or corrupted by such fluctuations. The long accepted solution to this is to insert batteries, uninterrupted power supplies and power generators between these components and the utility company power supply. This insertion is not always done and batteries fail. Because DREs are more electronic than any other voting technology (other than Internet voting), they are at greater risk of failure due to power issues. By comparison, punch-card systems are entirely mechanical and have no power failure issues for voting. Similarly, optical scan systems also enable voting without the need for electrical power (i.e., paper optical scan ballots are filled out manually by the voter). There are industry-accepted practices to mitigate the failure of electronic equipment due to power failures.

2.1.1.2.2 *Hardware Failures*

The equipment can have defects in design and manufacture that cause the hardware to fail under use or misuse. DREs are more electronic and as such have more complex and sensitive

¹ This also applies to the use of marking pens and optical character recognition (OCR) paper ballots currently used in Arizona. Optical scan counting equipment is electronic, but the voting process can continue without this equipment if necessary.

² Microprocessors, diodes, transistors and related components.

components than other types of voting technology. Electronic components are susceptible to environment conditions, such as excessive heat or cold, humidity, impact shock, etc. This makes DREs more vulnerable than other voting technologies to hardware failures. All these vulnerabilities can be mitigated with good technical design and equipment maintenance support practices.

2.1.1.2.3 Software Failures

The software may have defects, inadequacies or even intentional inaccuracies. Software is complex logic that requires rigorous discipline in its creation. Consequently, it is relatively easy for it to have errors or to encounter unanticipated operation. In addition, software is plastic; it can be easily altered by knowledgeable persons with access to it. Alterations are only limited by processor power and programmer imagination. Alterations could include clever disruption or deception regarding vote recording and vote tallying. This is more true of DREs than of other (except Internet voting) technologies for voting. There exists a large body of knowledge and best practices to prevent or address software failures. Implemented rigorously, these practices reduce the risk of software failure substantially.

2.1.1.2.4 Data Communications Failures

The equipment may have data communications failures, resulting in the inability to report results in a timely fashion. DRE (and optical scan equipment) can report vote tallies very rapidly via common dial-up connections. It is possible that without strict security protocols, these connections could be unreliable.

2.1.1.2.5 Training Failures

As with any technology-based business solution, equipment could fail due to incorrect configuration and installation due to inadequate staff training. Because DREs are more complex and more electronic, they have been perceived as more difficult to maintain, configure and install. The view is that the largely senior voting volunteers may have greater difficulty with these machines than with more traditional voting equipment. Anecdotal evidence gathered by Gartner, coupled with secondary research, does not support this. In fact, the County of Los Angeles (among others) works with the AARP to recruit poll workers from the senior population. The introduction of any new method will have a learning curve that is not always initially grasped by everyone.

2.1.1.3 Benefits of DRE

In addition to the many types of failures to which DRE systems are vulnerable, they also provide many advantages that other technologies do not offer or do not offer as well. DREs:

- 1) Have greater capacity and flexibility for ballot creation and revision
- 2) Eliminate much of the paper costs of ballot production, distribution, storage and destruction
- 3) Enable voters with visual impairments to vote a secret ballot
- 4) Reduce or eliminate the problems of over and under voting
- 5) Enable faster vote recording and vote tallying

The essential question is whether the overall benefits gained from using DREs outweigh the probability of failure and the negative consequences of such failure. DRE voting systems can only

be used appropriately to the extent that the probability of equipment failure can be significantly diminished, and the negative consequences of such failure quickly mitigated, all the while meeting high accuracy expectations.

2.1.1.4 Recommendations

Over 99 percent of Arizona voters currently use optical scan technology, not DRE technology to vote. Thus, this issue is of much less importance to Arizona than it is to many other states that rely entirely, or almost entirely, on DRE voting equipment. Arizona does have some DRE equipment currently deployed, and may need to acquire additional DRE equipment to meet accessibility requirements of visually impaired voters. For that very limited pool of devices, we would make the following recommendations:

- 1) Power Failures — The State should provide uninterruptible power supply (UPS) systems with each DRE device to ensure their continued operation (or safe shutdown) in case of a power failure.
- 2) Hardware Failures — The State should ensure appropriate environmental conditions and treatment for DRE equipment in accordance with their electronic nature.
- 3) Software Failures — The State should:
 - a) Apply a stringent certification process to each vendor's DRE software.
 - b) Require authentication that software that has been rigorously reviewed has not been subsequently altered.
 - c) Pressure DRE vendors to comply with industry best practices regarding software development, testing, distribution and version control.
- 4) Data Communications Failures — The State should use a number of transmission security techniques such as encryption, restricted dial modems, voice confirmation of transmission and other practices to minimize possible communications failures.
- 5) Training Failures — The State should ensure adequate training on the use of new DRE equipment both for poll workers and for voters.

2.1.2 Is VVPAT Required to Ensure that The Vote Cast Is The Vote Recorded?

2.1.2.1 Description

There is a question whether the vote cast with a DRE system may not be the vote that is recorded.

At present, nearly all voting in Arizona is done using optical scan technology, not DRE technology¹. Voter Verifiable Paper Audit Trail (VVPAT) is not an issue for optical scan technology, since the paper optical scan ballot sheet is considered a reliable VVPAT. VVPAT is only relevant to Arizona to the degree that it may be necessary to acquire DRE equipment to address the 2006 HAVA requirement to enable voters with visual impairment to vote a secret ballot.

¹ Yavapai County currently has ten (10) DRE machines that are used only for early voting. The early voter has a choice in Yavapai whether to use the DRE or cast their vote using the traditional optical scan ballot.

With an electronic process of vote recording, there is no visible means by which the voter can verify that the vote cast was, in fact, recorded and counted as cast.

One proposed solution to this problem for DRE systems is the simultaneous production of a VVPAT, which is a print-out of the vote cast, viewable (and therefore verifiable) by the voter, but stored for counting and later made available as an artifact of the vote should a recount be required. In such a circumstance, the VVPAT becomes the new “source of truth” document for the recount.

2.1.2.2 Analysis

2.1.2.2.1 What is Accuracy?

The question seeks assurance that every vote cast is counted as cast. Perhaps contrary to popular belief, there has probably never been a major election in which this has been 100 percent true in the past. There have always been votes cast that were never counted due to a variety of reasons. For example, as recently as June 2004, an election audit in Sioux Falls, South Dakota determined that paper ballots could be lost, stolen, damaged, altered and misread. Thus the concern is not so much that electronic systems are less accurate or reliable than paper ballots or punched cards, but simply that there is a goal that vote casting and vote counting be as accurate as possible. Further, the goal is that voters have confidence that “by and large” votes cast are votes counted and more importantly, there is no mechanism by which votes can be surreptitiously altered before counting.

2.1.2.2.2 Two Sources Means Two Counts

There is a maxim in the IT industry that if there are two sources for data, there will inevitably be two disparate results. Human systems are not perfect. If DRE equipment collects and counts votes and a VVPAT prints these votes which are then collected manually, it is highly likely that a recount will reveal a result that is not 100 percent identical to the result tallied electronically. Given this reality, it is not clear that the addition of a second source (a VVPAT) will improve voter confidence in election results. Clearly, as with any artifact (i.e., punch cards) the rules regarding a recount of artifacts must be established before the election and must be agreed upon and applied uniformly in the process of recount. Even so, a VVPAT does not hold the same promise of accuracy that is generally attributed to it.

2.1.2.2.3 Paper Costs

One of the reasons many election directors found electronic voting devices (DREs) attractive was that they eliminated many of the sizeable costs associated with using paper, e.g., printing, transportation, storage, etc. A VVPAT requirement puts them back in the paper business, though not to the same level of costs that exist with paper, punch card or optical scan ballots.

2.1.2.2.4 Who Can Verify the Systems?

There are really three questions embedded in this issue.

1. *Is It Sufficient If Current Systems Have the Confidence of Informed Persons? Are current electronic systems designed and built in such a manner that informed people would agree that they render the vote cast as the vote recorded with a very high probability?*

This is clearly not the case. Most current voting systems do not have the internal logic safeguards now considered by IT security specialists as sufficient to ensure their reliability and safety from intended or unintended disruptions.

2. *Is It Sufficient if New Systems Could Have the Confidence of Informed Persons?* If current electronic systems are not so designed, can electronic systems be designed in such a manner that informed people would agree that they render the vote cast as the vote recorded with a very high probability?

There are a number of security techniques that are routinely applied to modern information systems. If applied to election equipment, these techniques can ensure that the vote cast is the vote recorded (with a very high probability). Such techniques include various symmetric and asymmetric encryption technologies; the use of digital signatures in a public key infrastructure (PKI); the use of highly structured application development; deployment and maintenance techniques such as those promulgated by the Capability Maturity Model (CMM) and the Institute of Electrical and Electronic Engineers (IEEE). Though electronic voting systems are likely to remain isolated from the Internet, they need to adopt and adapt many of the security techniques currently employed to manage safely billions of financial and other transactions that currently transfer across the Internet¹. It would appear that this is feasible and even likely to occur in a decade or two from now. It could not be made universal in time for the 2004 Presidential election.

3. *Is It Sufficient Only If Systems Have the Confidence of the Average Person?* Even if current systems were designed or new systems could be designed in such a manner that informed people would agree that they render the vote cast as the vote recorded with a very high probability, would that be sufficient? Is it necessary that the average person who is not informed needs to be convinced from evidence they can see and understand, that the vote cast is the vote recorded?

When framed in this light, it is clear that the question is not one of technology, but of trust. Can all of the average persons trust the informed persons? If they can, they must also trust the mechanisms that determine who the informed persons are. What is at stake, however, is the ballot, the mechanism by which the democratic process is maintained and by which all public servants are held accountable.

All of Arizona's 15 counties use optical scan systems as their primary voting technology. Yavapai County has 10 DREs for early voting. To meet HAVA requirements for 2006, the state will require that at least a single accessibility device at each voting location will be provided for the sight- and mobility-impaired to enable these voters to vote a secret ballot. Such units could also perform "double duty" if they have a VVPAT attached to them. Voters who would like to use a DRE could do so without concern about its veracity since it would have the VVPAT feature.

2.1.2.2.5 How Much Confidence Is Enough?

If a VVPAT is required at this time, what level of this verification is necessary to garner the confidence of the average person?

¹ Existing examples include ATMs and electronic gaming (gambling) machines.

The RABA Study concluded that some degree of VVPAT is required at this time to ensure voter confidence. The RABA Study further suggested that perhaps 100 percent VVPAT is not required to establish voter confidence:

Indeed, if all AccuVote-TS terminals are checked to ensure they are functioning correctly before an election, and if they are loaded with identical, digitally-signed, software which is checked both before and after an election, one can make the case that reconciling the results of a single, randomly selected, terminal with its paper receipts is sufficient to believe that the overall electronic counts in that precinct are accurate. Thus, if all the terminals are software and hardware enabled for receipts, one need only provide receipts for a small number of randomly chosen machines. Voters might even be given the choice of using such a terminal — or not.

Even if RABA is correct, it appears that their observations are being overtaken by events. The states of California, Nevada and Ohio are requiring that all DRE systems produce a VVPAT. In addition, there is Federal legislation being crafted that would require a VVPAT nationally.

Despite movement toward VVPAT, it should be recognized that there is no guarantee that what is printed on the VVPAT is in fact what is recorded in the electronic memory of the DRE. Thus, the VVPAT is technologically no guarantee of veracity. That guarantee of veracity must come from the monitored methods and procedures of software development, testing, management, distribution and acceptance. The source of truth documents for Arizona should be the OCR and mail-in ballots used for voting (by 99 percent of Arizona voters) and the paper tape required by HAVA that is stored inside each DRE machine. Accordingly, Arizona should not acquire VVPAT unless required by law. It should require that all future DREs purchased come equipped with the capability to add a VVPAT if required.

2.1.2.3 Recommendations

There is no need for a VVPAT with the optical scan systems used by over 99 percent of Arizona voters, since the paper ballot serves the same purpose and can be hand counted if necessary. VVPAT usefulness is still being debated. Arizona should not adopt VVPAT for its limited population of DREs unless required by federal mandate.

2.1.3 Are Election System Firms Overcharging to Retrofit for VVPAT?

2.1.3.1 Description

There is a question whether electronic voting equipment vendors are overcharging their clients in order for them to meet state requirements for a VVPAT, especially when this involves retrofitting previously purchased systems.

The State of California requires that, effective July 1, 2005, counties will not be able to purchase any voting systems that do not produce a paper trail. The State also requires that as of July 2006, all machines, no matter when they were purchased, must offer a Voter-Verifiable Paper Audit Trail (VVPAT). This means that machines currently in use by four California counties will have to be fitted with new printers to meet this requirement.

2.1.3.2 Analysis

2.1.3.2.1 Cost of Retrofit

It will cost additional money to retrofit currently deployed DRE voting systems with the capacity to produce a VVPAT. This is especially true for the DREs that were not originally designed to accommodate printing.

Cost estimates for requiring VVPAT for systems that have been deployed vary. Alfie Charles, a vice president at Sequoia Voting Systems, estimated that VVPAT printers would add about 15 percent to the cost of voting machines. For California, therefore, this retrofit could be about \$60 million of the \$400 million California counties are expected to spend to comply with court orders and new federal requirements¹.

Administrator Linda H. Lamone of the State of Maryland Board of Elections told *The Gazette* that Diebold had given a preliminary estimate of \$1,000 to \$1,200 per machine to add printers, or up to \$20 million for the State's more than 16,000 machines. According to the article, “[Lamone] said that she could not recall whether she got the figure from Diebold or media reports”².

Palm Beach County, Florida is using Sequoia's DRE voting systems and will be requiring paper printouts of votes cast. Since it would cost money to retrofit Palm Beach County's existing machines to work with the new printers, Charles said, a printer would cost about \$600 with installation — \$3.24 million for the County's 5,400 machines. Each touch-screen machine costs about \$3,100.

California has invested more than \$139 million on electronic touch-screen technology. Secretary of State Kevin Shelley estimated the cost of adding capabilities to print a paper receipt from existing voting machines at \$1 million for California counties, except for the four counties which Shelly has barred from using their existing DRE equipment.

2.1.3.2.2 Impact on Arizona

Should this become a requirement, it will not have the impact on Arizona that it will have on many other states. All Arizona counties use optical scan for both regular and early voting. Only Yavapai County has DRE voting machines (10) for early voting. In the last election, 1,500 Yavapai voters chose to use this equipment. Thus, over 99 percent of voters in Arizona use optical scan technology to vote. Considering this, the VVPAT issue, is relevant to less than one percent of the State's voters. To retrofit these 10 machines with VVPAT (at \$600 per machine), would cost about \$6,000.

Beginning in 2006, all Arizona counties will have a requirement to provide systems that enable the disabled to cast a secret ballot. A very common solution to this problem is the use of DRE equipment that enables a vision-impaired person to hear contest choices and make a selection and then hear confirmation of their selection. Should Arizona determine that DREs are the best alternative for vision-impaired secret ballots, then it is likely that VVPAT would be added to these

¹ “State Tells Counties to Establish Paper Trail on Electronic Voting”
<http://www.latimes.com/news/local/la-me-shelley21nov21,1,3417363,print.story>

² “E-mail stolen from Diebold is a call to gouge Maryland”
- <http://www.gazette.net/200350/montgomerycty/state/191617-1.html>

systems to allow any voter to use them with confidence in the result. It may be possible to address the concerns of the visually impaired community by allowing voters to turn the VVPAT off while they cast their ballot. DREs may also be outfitted with VVPAT in accordance with a sampling confidence approach as discussed elsewhere in this report.

2.1.3.3 Recommendations

- 1) There is fear, but little evidence, that voting system vendors are “price gouging” because of emerging requirements for VVPAT. However, there is no specific requirement that the vendor be the one to add the printer to the equipment. The printer could be added by a third party under a separate contract.
- 2) The State should ensure that if a DRE solution is chosen to meet HAVA disability requirements for 2006, the solution is configured to enable the connection of a printer as necessary to create a VVPAT.

2.2 Questions Regarding Certification

2.2.1 Does the Federal Certification Process Adequately Examine System Security?

2.2.1.1 Description

Federal testing and certifications were originally focused on the accuracy and reliability of voting equipment but not as focused on security protection against emerging electronic types of threats. It appears that there has been no extensive analysis by the federal testing and certification authorities of the software source-code being used in the newer DRE systems and that software is not critically examined to find security flaws and potential programming anomalies that could possibly alter the accurate recording of election counts.

2.2.1.2 Analysis

2.2.1.2.1 Pre-HAVA FEC Voting Standards (2002)

“On April 30, 2002, the Federal Election Commission (FEC) approved new Federal Voting Systems Standards (FVSS). The Standards are divided into two volumes.

- Volume I provides performance standards and functional capabilities for voting systems that are seeking Federal qualification.
- Volume II addresses documentation required to be submitted by the vendor prior to testing, it defined to be conducted by the Independent Test Authorities (ITAs), and the products generated by the test process.

The standards include performance standards for security that describe essential security capabilities for a voting system, encompassing the system’s hardware, software, communications, and documentation. The objectives of the security standards for voting systems are:

- To establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized;

- To protect the system from intentional manipulation and fraud, and from malicious mischief;
- To identify fraudulent or erroneous changes to the system; and
- To protect secrecy in the voting process.

While the testing standards provide standards for examining software source code, they do not define explicit procedures for testing the security aspects of a vendor's source code."¹

Under FVSS, the Federal Elections Commission (FEC) formulates, maintains and revises voting systems standards to keep changes in technology and testing requirements current. The FEC coordinates with the National Association of State Election Directors (NASSED) to assure that independent testing can be performed under the standards. No voting system is ever "Federally Approved" or "FEC Approved."

NASSED selects and approves testing laboratories that perform testing related to voting systems to meet the FVSS. The standards are not NASSED standards and NASSED does not have authority over the FVSS. NASSED selects and qualifies Independent Test Authorities (ITAs) to perform the work of professional testing to assure that voting systems manufacturers comply with the FVSS. NASSED has no ability to determine whether a system passes or fails. ITAs operate independently to determine objectively whether the vendor has met or exceeded the FVSS. When a system passes testing through a qualified ITA, the ITA informs NASSED of its compliance and then NASSED issues one or more numbers which identify to the states that the system has been qualified by NASSED.

Independent Testing Authorities (ITAs) perform professional testing to assure that voting systems comply with the FVSS.

The Election Center serves as NASSED's day-to-day management company for working with the ITAs, with the FEC and with the states. The Center has no authority to pass or fail any system, but works with the local jurisdictions in answering questions concerning the manufacturers' products that have been qualified (or not qualified) under the FVSS. The Center serves as the focal point for coordination among the FEC, NASSED and state and local jurisdictions and the ITAs.

2.2.1.2.2 HAVA Voting Standards (2003)

"In December 2003 the Election Assistance Commission (EAC) was created as a result of the Help America Vote Act (HAVA) of 2002. The EAC takes over some of the roles of the FEC and will serve as a national clearinghouse and resource for gathering information and reviewing procedures with respect to the administration of Federal elections. In addition to its advisory role, the EAC is responsible for carrying out duties related to the testing, certification, de-certification, and re-certification of voting system hardware and software.

Part of the charter of the EAC is to study and report on Electronic Voting. The study will include an examination of the appropriate security measures required and

¹ http://www.nist.gov/public_affairs/factsheet/voting_symposium.htm

minimum standards for certification of systems or technologies to minimize the potential for fraud in the voting or registration process. Preliminary reports from the EAC, however, indicate it will not be able to address immediately this part of its charter due to funding issues.

HAVA also gives the Commerce Department's National Institute of Standards and Technology (NIST) a key role in helping realize nationwide improvements in voting systems by January 2006. NIST is the chair of the Technical Guidelines Development Committee, which makes recommendations to the EAC on voting machines standards. NIST's Information Technology Laboratory (ITL) is coordinating the agency's HAVA efforts through its expertise in areas such as computer security and usability. According to NIST, no standards based on any federal recommendations will be in place before the 2004 national elections."¹

ITL has already started research in this area, releasing a report in May 2004 on "*Improving the Usability and Accessibility of Voting Systems and Products*." The activities to develop these new standards, however, have yet to be funded.

2.2.1.3 Recommendations

- 1) If Arizona proceeds with expanded deployment of DRE technology and Federal standards and guidelines addressing DRE security are not available, Arizona should develop its own certification procedures to address these issues².
- 2) See recommendations in this report regarding certification procedures best practices regarding security testing.
- 3) The State should aggressively work with NIST to ensure that the State's protocols and procedures align with national standards as early as possible.

2.2.2 Do States Need to Conduct Testing Beyond Current Federal Certification Requirements?

2.2.2.1 Description

The states (including Arizona) primarily rely on the federal certification process, but since the federal certification process does not currently focus on issues such as security, should states (including Arizona) conduct additional comprehensive independent certification of equipment to be used within the state?

2.2.2.2 Analysis

Current federal testing and certification procedures especially for DRE voting systems are not comprehensive enough to ensure the full security integrity of a vendor's system. This would imply that states need to generate rigorous security standards and require the vendors to produce evidence of independent analysis of their source code to fill the gap in federal-level security testing. Under HAVA, NIST is charged with developing these new standards, and therefore, efforts by the

¹ http://www.nist.gov/public_affairs/factsheet/voting_symposium.htm

² See the Appendix of this report regarding best practices certification procedures.

states in this area may prove to be premature. Unfortunately, however, the new standards function of NIST has not yet been funded by the federal government, and therefore, the time frame of these new federal-level standards is uncertain.

2.2.2.3 Recommendations

- 1) The State should conduct its own certification testing for its unique requirements (e.g., the Arizona/Wyoming Ballot Rotation).
- 2) The State should lobby the EAC for better security guidelines and testing standards, and the ITAs for better testing protocols and documentation¹.

2.3 Is The Enfranchisement of the Disabled Being Delayed?

2.3.1 Description

HAVA requires that by 2006, states facilitate independent voting by the disabled using electronic voting devices. The issues are that:

- 1) Disabled voters may vote, but are unable to cast a secret ballot.
- 2) There is technology now that would enable them to cast a secret ballot.
- 3) Waiting until 2006 is further denying them their civil right to a secret ballot.
- 4) Disabled persons (particularly the visually impaired) will not be able to use the VVPAT and still maintain a secret ballot.

2.3.2 Analysis

Some states promised to provide equipment for disabled voters in time for the upcoming 2004 General Election. Many of them have found it necessary to retract those promises and are now proposing to meet the Federal 2006 requirement deadline. This has irritated many in the disabled community who feel that there is no reason to delay until 2006. James C. Dickson, Vice President for Governmental Affairs at the American Association of People with Disabilities, stated in his testimony to the U.S. Senate, "The disability community's patience, as we wait for polling places and voting systems to be made accessible, is running thin."²

Arizona plans to meet the Federal 2006 requirement deadline and continues to work toward that goal. Arizona is currently conducting a pilot project and will continue to work with the disabled community to ensure that a quality solution for accessible voting is obtained.

2.3.3 Recommendations

Arizona should continue to work to comply with the Federal 2006 requirement to provide secret ballot capability to the disabled at each polling location through the deployment of an accessible voting device. Accessible voting devices include DREs and alternative technologies that operate like DREs, but record votes on scannable paper documents.

¹ See the Appendix of this report regarding best practices certifications processes.

² James C. Dickson comments to US Senate http://rules.senate.gov/hearings/2001/062701_dickinson.htm

2.4 Should All Source Code Used in Elections Be “Open”?

2.4.1 Description

The source code used in election systems is generally not available for review by knowledgeable persons independent of the vendor of the system. Review may help ensure quality software code, detect flaws or necessary omissions, and improve voter confidence and trust in the accuracy of the voting and vote counting process.

An analogy is drawn with Linux open source, which is seen as a “tried and true” method of ensuring software security, since all potential vulnerabilities that the manufacturer may have overlooked are caught and scrutinized publicly. There is some question as to whether voting source code should be public or simply available to independent, professional scrutiny.

2.4.2 Analysis

There are two essential questions:

- 1) *Should Third Party Review Be Required?* — Should election system software be made available for review by third-party independent reviewers?
- 2) *Should Public Review Be Required?* — Should election system software be made available to the public (published as Open Source code)?

2.4.2.1 *Third-Party Review*

Third Party Review by ITA — The ITAs authorized by FEC have access to the source code of election system commercial software developers. Thus, third-party review of election system commercial software is already a fact.

Third-Party Review by Customer Request — Commercial software developers have reason to maintain the confidentiality of their source code to ensure propriety business advantage over their competitors. Commercial software developers, however, do provide source code for examination by their customers if a non-disclosure agreement is signed. Diebold makes its source code available to customers who want it independently audited. According to Diebold:

“Diebold Election Systems has and will continue to open up its system for review by respectable, unbiased, third-party experts such as those evaluations conducted in Maryland and Ohio. We are confident in the integrity and security of our system, and that the electronic voting format holds the greatest potential for ensuring impartial, secure and accurate elections.”¹

Third-Party Review by States, Commission or Universities — The third-party review that does not now occur is third-party review by the states, commissions or universities. Various commissions may have reason to review code and universities have knowledgeable persons with an interest and a contribution to make. States, however, have a direct and vested interest in the quality of election software and are responsible for the conduct of accurate and timely elections.

¹ <http://www.diebold.com/dieboldes/ohio.htm>

2.4.2.2 Public Review

Open source generally implies that the code is available for review by anyone, anywhere and that it is typically published on the Internet for such availability. This level of exposure would permit competitors to ascertain exact methods and techniques of their competition, thus rendering superior application development no longer a competitive edge. More importantly, it would make it possible for anyone who understands the system's vulnerabilities to subvert the system. On balance, there would seem to be little public good gained from such exposure.

2.4.3 Recommendations

- 1) The State should require that all software source code be held in escrow and made accessible to qualified state staff if and when necessary.
- 2) The State should test for those requirements that are relatively unique to Arizona such as the Arizona/Wyoming Ballot Rotation algorithm
- 3) The State should lobby for the adequate allocation of resources to NIST and ITA to ensure that they fulfill their mission of adequate functional and security testing of election systems.
- 4) The State should place in its RFPs and contracts that all system software source code is subject to review by experts at the state's discretion.

3.0 Questions Regarding Current Diebold Election Systems

Although Diebold has been in the news as the center of much of the concern regarding new voting technology and Arizona has purchased voting technology from Diebold, a very fundamental distinction should be made. The controversy is around DRE technology, while Arizona purchased optical scan technology as its mainstay voting technology. This was a very prudent decision on the part of Arizona, as many states were acquiring the more attractive DRE technology at that time¹. Arizona wisely determined that the less high-tech, paper-based optical scan technology was the safer, more reliable and more voter-verifiable technology. This has proven to be true. The Arizona decision-makers in this instance should be recognized for making a wise decision on the selection of voting technology. This decision has enabled Arizona to largely avoid many of the voting systems issues that have been in the news and which are discussed in this report regarding (Diebold) DRE technology.

3.1 Do Current Diebold DRE Election Products Have Security Flaws?

3.1.1 Description

The question is whether Diebold voting systems have security flaws that can be exploited by an internal or external party to compromise election results.

3.1.2 Analysis

3.1.2.1 Major Recent Studies

Numerous independent studies have been conducted to examine the security of Diebold election systems. Some notable studies are:

- 1) *Johns Hopkins University Study*, July 2003² — Johns Hopkins University Information Security Institute conducted a study on Diebold voting system source code, which it found on a publicly accessible Diebold FTP³ site, and subsequently posted it on the Internet. The study noted significant security flaws of the purported source code for the Diebold AccuVote-TS voting system.
- 2) *State of Ohio Compuware Report*, November 2003⁴ — This report was commissioned by the Ohio Secretary of State to assess the security and validation assessment of the DRE voting equipment that had been certified by the Secretary of State for operation in Ohio. These were:

¹ Los Angeles County, perhaps the single largest voting operation in the country, was considering the same decision at the same time and decided to not acquire DRE equipment but instead to go forward with an optical scan solution. They now report great satisfaction with that decision.

² "Analysis of an Electronic Voting System", Information Security Institute, John Hopkins University, 23 July 2003.

³ FTP is File Transport Protocol, a UNIX public domain utility for file transfer.

⁴ "Direct Recording Electronic (DRE) Technical Security Assessment Report" by Compuware Corporation of Columbus, Ohio, November 2004.

- a) Diebold Election Systems — AccuVote-TS
- b) Election Systems and Software (ES&S) — iVotronic
- c) Hart InterCivic — eSlate 3000
- d) Sequoia Voting Systems — AVC Edge

This report reviewed the intended operation of each of these systems and made recommendations for their use within Ohio.

- 3) *State of Maryland SAIC Study*, September 2003 and January 2004¹ — State of Maryland commissioned a Risk Assessment Study by SAIC. The assessment was conducted by SAIC on behalf the State of Maryland just before the State award of \$55.6 million to acquire a new Diebold system. The Report recommended an "action list" of 23 items to be undertaken to secure the machines. The State expressed confidence in the system but came under pressure to conduct a second study².
- 4) *State of Maryland RABA Study*, Jan. 2004³ — A second review was commissioned by the State and conducted by RABA Technologies. The second study for the State of Maryland was conducted by RABA Technologies and reviewed the SAIC Study Report. The RABA study was an independent "Red Team" review. The RABA Report produced near-term recommendations to improve the system that can be implemented so the machines can be used for the March 2004 primary⁴.

The RABA report is quite recent, was built upon the findings of the prior reports, but went beyond them in very significant ways. The RABA report concluded that the Diebold election systems had significant security flaws as follows:

3.1.2.2 DRE Smart Card Security Flaws

Diebold uses the same smartcard hardware for the following functions:

- 1) *Voter Access* — Given to each voter for insertion into voting equipment. Ensures that voter receives the correct electronic ballot
- 2) *Supervisor Access* — Held by election officials to perform initialization, and shutdown and results transmission
- 3) *Security Key Card* — Allows election officials to change the default passwords used to secure the supervisor and voter cards

These functions are password protected. The password and the function are placed on the card by use of an Encoder Device.

¹ "Risk Assessment Report of Diebold AccuVote-TS Voting System and Processes", by Science Applications International Corporation (SAIC), 2 September 2003.

² "State of Maryland Voting Machine Risk Assessment" - www.dbm.maryland.gov/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf

³ "Diebold AccuVote-TS -Voting System Security Action Plan", 20 January 2004

⁴ "Trust Agent Report", Diebold AccuVote-TS Voting System - <http://www.raba.com/press.html?id=9>

RABA and Compuware found that in DRE equipment the password for each function was “hard-coded” in the application logic, making them uniform for all installations of this Diebold equipment. At the time of testing, the RABA team was able to guess the hard coded password and was able to duplicate a voter card and change it into a supervisor card. RABA has claimed that this could be done at a polling place using a compact PDA.

Diebold has stated¹ that default passwords were hard coded for testing purposes only, and that these defaults should to be replaced by values selected by the state or local jurisdiction before use of the equipment. Diebold states that no one, including Diebold, can have access to these passwords once they have been changed by the election officials.

At the time of this test, the contents of these cards were neither encrypted nor digitally signed. Diebold states that production ready smart cards are now protected by strong encryption and that no data can be written or read from a card without having the 64-bit encryption key. Trying to guess the results would result in permanently destroying the cards.

RABA DRE SmartCard Recommendations:

- 1) Create Security Key Cards with computer-generated passwords *by precinct*. Update all the Encoders and AccuVote-TS terminals within each precinct.
- 2) Apply Tamper Tape² to AccuVote-TS terminals to prevent non-authorized entry of Security Key Cards into the terminals.
- 3) Institute strict procedures to prevent the use of unauthorized Supervisor Cards.

3.1.2.3 AccuVote-TS Terminals

3.1.2.3.1 Components

The AccuVote-TS terminals consist of both hardware and software components that interact to produce ballots and register votes.

The hardware consists of a touch-screen voting terminal with two locked bays.

- 1) One bay houses a roll of paper tape that prints out the initial (“zero count”) vote tally and, following the election, the final vote tally.
- 2) A second bay houses:
 - a) The on/off power switch
 - b) Two (2) PCMCIA slots
 - i) For the flashdisk card that holds the ballot definition and records votes cast
 - ii) For the modem
 - c) A standard keyboard jack.

¹ Diebold Letter to Craig Stender, Arizona HAVA Project Manager, regarding review of draft of this Gartner Report, 20 August 2004.

² A physical indicator that ensures that the protected item has not been opened or disturbed.

3.1.2.3.2 Bay Access

“During an election, the bays are locked. Maryland has ordered approximately 16,000 AccuVote-TS terminals each equipped with two locking bays and supplied with two keys accounting for 32,000 locks and keys. Each lock is identical and can be opened by any one of the 32,000 keys. Furthermore, team members were able to have duplicates made at local hardware stores. It is a reasonable scenario to assume that a working key is available to an attacker.”

During the RABA study, the bay locks could be picked in approximately 10 seconds. Some precincts load their terminals the day before the election, and therefore, the opportunity to access these bays may be possible both before and during an election.

Diebold notes¹ that its newer machines have stronger locks and that these are only a small part of the overall physical security that should be deployed wherever the machines are stored. In addition, access to the cards is still prevented by encryption and digital signatures.

3.1.2.3.3 Possible Attacks

RABA discovered and demonstrated the following types of attacks:²

- 1) By keyboard
- 2) By removal of the PCMCIA card
- 3) By file update to a PCMCIA card
- 4) By installation of new passwords
- 5) By jamming the card reader
- 6) By disconnecting the monitor

“These are a sampling of the vulnerabilities found as a result of poor physical security coupled with software that fails to use robust encryption and authentication. The team feels confident that physical access to the bay housing the PCMCIA cards, power switch, and keyboard jack can ultimately lead to devastating results to the particular terminal. Most of the near-term recommendations focus on securing this bay.”

It should be noted that the risk of attacks should be put in the context of a properly set up system similar to that typically done on Election Day. Most of the vulnerabilities can be mitigated by enhancing procedures around the setup of the polling place where vigilant physical security of the polling place should prevent vandalism. In these situations, physical attacks would be detected immediately.

Diebold states¹ that it is important that attacks be detected and that neither RABA nor anyone has demonstrated any successful attack on a properly set up system. Diebold also notes that what has

¹ Diebold Letter to Craig Stender, Arizona HAVA Project Manager regarding review of draft of this Gartner Report, 20 August 2004.

² See RABA Report for details about each type of attack.

been missing from laboratory-originated tests has been the real-world experience of the voting booth, including the people and the rigorous procedures that are in place to conduct the election safely and securely.

3.1.2.4 RABA DRE AccuVote-TS Terminals Recommendations:

- 1) Secure physical access to the voting terminal. The team recommends the use of serial-number tamper tape placed both inside and outside each locked bay. This could be accomplished in the following manner: After the terminals are loaded and a zero-tape printed, the bay doors would be secured with the tamper tape and the serial numbers would be recorded. The tamper tape would need to be inspected periodically as a matter of procedure. Ultimately it would be recommended to place alarms on the bay doors.
- 2) Remove the test recording software from the AccuVote-TS terminal that allows the keyboard exploit. It serves no valid function.
- 3) Investigate the legal implications of tampering with the hardware systems (such as jamming the card reader and disconnecting the monitor). We see no short-term fix for these attacks aside from the clear posting of rules that indicate consequences of such actions.

3.1.2.5 GEMS Security

In addition to voting equipment, Diebold provides central count equipment. This is a server running Diebold's Global Election Management System (GEMS) software. GEMS is run by each local election district (county) and by the state elections officer (secretary of state). These systems are normally not connected to any networks but are briefly connected via modem for the transmission of election results.

The RABA Red Team demonstrated the following GEMS vulnerabilities²:

- 1) Remote vulnerability via modem
- 2) Physical access vulnerability via USB
- 3) Physical access vulnerability via CD
- 4) Database vulnerability
- 5) Remote access vulnerability by spoofing central count
- 6) Lack of firewalls, default no access, missing patches and updates

RABA states that these vulnerabilities demonstrate considerable and often obvious security oversights by Diebold and that it is apparent that there has not been a concerted, planned security review and development but only ad-hoc implementations of some security controls.

RABA GEMS recommendations:

- 1) "Install all known security patches from Microsoft on the GEMS servers.

¹ Diebold Letter to Craig Stender, Arizona HAVA Project Manager regarding review of draft of this Gartner Report, 20 August 2004.

² See RABA Report for details regarding GEMS vulnerabilities.

- 2) Ensure modem access to GEMS is enabled *only when uploads are expected*. The [telephone] number used for this purpose should be *guaranteed* not to change. Shut off the modems when not in use.
- 3) Turn off all services and ports except those explicitly required by the GEMS software. For defense-in-depth, install firewall software to block all ports except those required by the GEMS software.
- 4) Update the anti-virus software.
- 5) Turn off services that are not needed by GEMS.
- 6) Install Tripwire¹ on the system to provide an audit capability on the configuration.
- 7) Disable the “autorun” feature in Windows 2000².
- 8) Ensure the front panel on the server is locked and the server is stored in a physically secure location. Apply tamper tape to the input devices and the reboot button.
- 9) Change the boot order to make the hard drive first and password-protect the BIOS to prevent changes to the boot order without physically opening the server.”

3.1.3 Recommendations

- 1) It should be remembered that the AccuVote-TS terminal described above is Diebold’s DRE solution. Arizona has purchased Diebold’s optical scan solution that has not been the subject of these security concerns. If Arizona decides to acquire Diebold DRE solutions (possibly in limited quantity for voters with disabilities), the State (in concert with other states) should continually press Diebold to correct the security vulnerabilities of this system.
- 2) The State should consider acquiring an alternative solution to the AccuVote-TS terminal for voters with disabilities, but such solution should be compatible with central count software currently being used by counties.
- 3) The GEMS central count software has been acquired by some Arizona counties including Apache, Pima and Yavapai. It is not practical to consider alternative central count products since GEMS is designed to work with the optical scan voting equipment acquired by these counties for voting. In addition, most of the RABA recommendations for securing the system can be accomplished by these counties without dependence upon Diebold. They represent good security measures for protecting most any Microsoft Windows server. Accordingly:
 - a) The State should allow Arizona counties that are currently using the GEMS central count software to continue to do so.
 - b) The State should encourage all Arizona counties using GEMS to also implement the RABA GEMS security recommendations:
 - i) “Install all known security patches from Microsoft on the GEMS servers.

¹ Tripwire is a change management control software product of Tripwire, Inc. <http://www.tripwire.com/>

² Change the value from “1” to “0” for the registry key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDRom

- ii) Ensure modem access to GEMS is enabled *only when uploads are expected*. The [telephone] number used for this purpose should be *guaranteed* not to change. Shut off the modems when not in use.
 - iii) Turn off all services and ports except those explicitly required by the GEMS software. For defense-in-depth, install firewall software to block all ports except those required by the GEMS software.
 - iv) Update the anti-virus software.
 - v) Turn off services that are not needed by GEMS.
 - vi) Install Tripwire¹ on the system to provide an audit capability on the configuration.
 - vii) Disable the “autorun” feature in Windows 2000².
 - viii) Ensure the front panel on the server is locked and the server is stored in a physically secure location. Apply tamper tape to the input devices and the reboot button.
 - ix) Change the boot order to make the hard drive first and password-protect the BIOS to prevent changes to the boot order without physically opening the server.”
- c) The State should closely monitor and encourage Diebold security enhancements to GEMS.

3.2 Are Diebold Products Vulnerable to Internet Attacks?

3.2.1 Description

Various reports indicate that Diebold election systems do not have modern software protections that would make them secure against various types of software attacks if they were connected to the Internet. Such attacks include “denial of service” attacks where the equipment is disrupted by massive transactional requests and virus attacks that corrupt the software or the information being processed.

Diebold states³ that Election System touchscreen units are standalone voting stations that are never connected to the Internet, therefore eliminating the risk of Internet hacking. In addition, they are also not networked within the precinct.

3.2.2 Analysis

A network port is provided on the AccuVote-TS to download ballot definitions and upload results. There is a risk that if the AccuVote-TS is connected to an unsecured Internet or Intranet, the AccuVote-TS could be compromised⁴. Furthermore, the network port could be exploited by a

¹ Tripwire is a change management control software product of Tripwire, Inc. <http://www.tripwire.com/>

² Change the value from “1” to “0” for the registry key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDRom

³ Diebold Letter to Craig Stender, Arizona HAVA Project Manager regarding review of draft of this Gartner Report, 20 August 2004.

⁴ Ohio Compuware Report, Page 78

person using a locally connected device within the voting booth to introduce new programs or changes to data.

As part of security enhancement efforts, Diebold has ensured¹ that all data transmissions to and from the voting terminal are encrypted using secure sockets layer (SSL). In addition, Diebold now uses SSL for all communications including uploads and downloads taking place within secure rooms at election central.

3.2.3 Recommendations

For all Arizona counties:

- 1) Do not connect voting equipment of any kind to the Internet or to an Intranet.
- 2) Do not allow equipment used for voting to have an alternate use during non-election times.
- 3) Include in pre- and post-election checklist a step to check that there are no cables attached to the network cards of any of the election equipment components including both precinct and central count locations.

3.3 Does Diebold Have A Quality Software Development Methodology?

3.3.1 Description

The question is: Does Diebold use best-practice software development methodologies that would help in ensuring that its software is of the highest quality and is built in a manner that minimizes security vulnerabilities?

3.3.2 Analysis

Diebold claims that their software development environment is ISO 9000 compliant. It is, however, not evident that widely accepted standards of software development, such as the Carnegie Mellon Software Engineering Institute's Capability Maturity Model (CMM)² for Software and System Security Engineering (SW-CMM and SSE-CMM), were followed in developing Diebold software³. CMM is set of guidelines and an assessment methodology for processes and controls on the development, testing and management of software. Although Diebold has apparently not followed industry-accepted standards for software development in the past, it should be noted that neither have many of the other election system vendors.

¹ Diebold Letter to Craig Stender, Arizona HAVA Project Manager regarding review of draft of this Gartner Report, 20 August 2004.

² For additional information regarding CMM, See: <http://www.sei.cmu.edu/managing/managing.html>.

³ Raba Report, Page 7

3.3.3 Recommendations

In all future contracts, the State should require all voting system vendors to secure Software Engineering Institute CMM Level 2 certification within one year and CMM Level 3 certification within three years.

- 1) CMM Level 2 ensures the vendor uses repeatable policies and procedures for managing a software development project and has instituted basic software management controls.
- 2) CMM Level 3 ensures a standard process for developing and maintaining software is documented and used across the organization. The process integrates both software engineering practices and management processes into a coherent process.
- 3) Organizations that have adopted the CMM have reported improvements in productivity and application quality as a result¹.

3.4 Do Diebold Products Have Adequate Configuration Management?

3.4.1 Description

The question is: Does Diebold use best-practice software management tools and methodologies that would help in ensuring that the software it develops is tightly managed and that “builds” are well defined and rollback is feasible and reliable?

3.4.2 Analysis

There have been examples where Diebold has placed software upgrades² or patches on machines without going through the certification process.

After a State of California investigation in November 2003, Diebold certification was made conditional. The audit discovered that the company had placed uncertified software on some touch-screen machines used in elections³.

There was also a case in Arizona where counties had to use previous versions of GEMS to run important reports, i.e., Statement of Votes Counted (SVC Report) because the current certified version could not run the reports⁴.

The examples above may indicate that Diebold has difficulty controlling or monitoring the configuration of its software applications.

3.4.3 Recommendations

- 1) The State should require CMM Level 2 certification.

¹ Ohio Compuware Report, Page 19

² An upgrade is defined as any change to a system’s software or hardware to correct or improve its operation.

³ “Diebold Gets Stay in California”, Wired News - <http://www.wired.com/news/evote/0,2645,61947,00.html>

⁴ Counties had to use version 1.1.8.15. for reporting instead of version 1.18.18.

- 2) The State should implement strict policies and procedures that ensure that only certified software upgrades and patches are made to election systems.
- 3) The State should require all patches and software are digitally signed by the vendor.

3.5 Do Diebold Products Have Adequate Password Management?

3.5.1 Description

Among revelations contained in the memos taken from Diebold was information that the Microsoft Access database used by the Diebold GEMS central tabulation system to collect and calculate votes was not protected by a password. This meant someone could alter votes by entering the database through physical access to the machine or remotely using a modem. In addition, it was revealed that many customers of Diebold do not change the default password in both GEMS and AccuVote-TS equipment, and that there are several key accounts and passwords that may or may not be known to customer/users of Diebold election systems.

3.5.2 Analysis

The original versions of the AccuVote-TS supervisor cards had an associated “hard coded” PIN password provided by Diebold. Diebold had set the password on all supervisor cards issued nationwide to “1111.”

- 1) There was a risk that an unauthorized person could learn the default PIN number and gain access to the supervisor functions on the machine. Further, any supervisor card will function on any DRE in any election¹. The existence and value of the PIN code was easily available.
- 2) It was possible for an attacker to create a Security Key Card due to the use of fixed passwords. An attacker could create a Security Key Card (with a password known only to him), insert it into the AccuVote-TS terminal, and change the passwords. That terminal would then reject all Voter and Supervisor Cards until it could be reset with the correct passwords².

GEMS Software uses Microsoft Access to store data used to create ballot definitions and tally results. Microsoft Access databases can be viewed and modified using widely distributed software such as MS-Access or MS-Excel.

There is a risk that a user with access to the GEMS server can access the database and change ballot definition and voting result records³.

It should be noted that these scenarios, while possible, are not easily executed due to security procedures that limit the exposure of the equipment and by the use of many other security controls.

¹ Ohio Compuware Report, Pages 57 and 78

² Raba Report, Page 19

³ Ohio Compuware Report, Page 79

It should also be noted that lack of password management has been an industry-wide issue, not one confined to Diebold. As a result of the media attention placed on Diebold password management, other voting system vendors have now also addressed this issue.

3.5.3 Recommendations

- 1) Should the State acquire AccuVote-TS Terminals, it should develop password management administrative policies and procedures to mitigate this risk. For example:
 - a) Create Security Key Cards with computer-generated passwords by precinct. Update all the Encoders and AccuVote-TS terminals within each precinct.
 - b) Apply Tamper Tape to AccuVote-TS terminals to prevent non-authorized entry of Security Key Cards into the terminals.
 - c) Institute strict procedures to prevent the use of unauthorized Supervisor Cards¹.
 - d) Ensure that the PIN be at least six digits in length².
- 2) The State should ensure that Arizona counties using GEMS eliminate group accounts and establish individual user accounts on their GEMS servers. The State should also ensure that they apply and enforce Access Control Lists (ACL) to their GEMS software and databases and enable system auditing to record and save ACL events³.
- 3) The State should require that the Arizona county GEMS servers use proper Windows security to prevent unauthorized access, and not contain any additional software that would allow access to the GEMS database⁴.
- 4) The State should ensure that all Arizona counties (including those not using Diebold systems), develop and maintain adequate password management.

3.6 Do Diebold Products Have Adequate Access Management?

3.6.1 Description

Access management is concerned with controls on access to computing resources. In this instance, it is concerned with access to Diebold voting and central count systems. There has not been controversy regarding Diebold's optical scan voting equipment security, which is the bulk of what has been acquired by the State of Arizona. We discuss extensively the access management of Diebold DRE voting equipment (AccuVote TS) in Section 3.1 Diebold Security Flaws. Here we review Diebold central count equipment (GEMS) access management.

¹ Raba Report, Page 17

² Ohio Compuware Report, Page 78

³ Raba Report, Page 24

⁴ Ohio Compuware Report, Page 79

3.6.2 Analysis

The GEMS database files that contain the election definition (and results) are neither encrypted nor authentication protected¹. Results can be modified at will. In addition, ballot definitions can be altered so that the mapping between candidates and their “ordinal numbers”² can be changed. A sophisticated user can automate this procedure requiring only a few minutes’ access to the server³.

3.6.3 Recommendations

- 1) Use a smart card as the authentication token rather than a user name and password for uploading results to the GEM server and for accessing the GEMS software on the server.
- 2) The dial-up Point-to-Point Protocol (PPP)⁴ authentication currently uses Password Authentication Protocol (PAP)⁵. We recommend challenge-response authentication protocol (CHAP)⁶.
- 3) Use encryption when transmitting votes from the AccuVote to the GEMS server to prevent “man-in-the-middle attacks”⁷.

3.7 Do Diebold Products Have Adequate Authentication of Election Reporting?

3.7.1 Description

The question is: Are Diebold systems lacking the full capabilities to authenticate the election results received at the central tabulation sites using Diebold’s central software system?⁸ This vulnerability

¹ Encrypted means encoded so that it cannot be read without access to a special key with which to decrypt the text. Authenticated means that it would require a login name and associated password before access would be granted.

² Ballot position

³ Raba Report, Page 21

⁴ PPP (**P**oint-to-**P**oint **P**rotocol) is the most popular method for transporting IP packets over a serial link between the user and the ISP. Developed in 1994 by the IETF and superseding the SLIP protocol, PPP establishes the session between the user’s computer and the ISP using its own Link Control Protocol (LCP). PPP supports PAP, CHAP and other authentication protocols as well as compression and encryption.

⁵ PAP (**P**assword **A**uthentication **P**rotocol) - The most basic access control protocol for logging onto a network. A table of usernames and passwords is stored on a server. When users log on, their usernames and passwords are sent to the server for verification. Contrast with [CHAP](#), which encrypts the username and password before transmitting it.

⁶CHAP (**C**hallenge **H**andshake **A**uthentication **P**rotocol), an access control protocol that dynamically encrypts the user’s ID and password. The logon procedure in the user’s machine obtains a key from the CHAP server, which it uses to encrypt the username and password before transmitting it.

⁷ “Man in the middle attacks” occur when a third party intercepts transmission and acts as one of the parties to the transmission.

⁸ Global Election Management System (GEMS)

would enable a third party to “impersonate” the central site, intercept election results, alter them and report altered results to the central site on election night.

3.7.2 Analysis

The chief security component in election result transmission is authentication¹. In electronic transmission of election results, the GEMS system requires a password from the AccuVote terminal, but the terminal does not require any authentication of the GEMS server. Therefore, it is readily possible for a precinct to unwittingly download its results (and password) to an anonymous laptop (pretending to be the GEMS server). The laptop could then modify the election results and upload them to the intended GEMS server, all in real time. Focusing on encryption may have unintentionally diverted attention from the more pressing vulnerabilities².

What is needed is two-way authentication in which the AccuVote terminal at the precinct is authenticated to the GEMS server and vice-versa before any transmission of election results is conducted.

One of the most secure electronic authentication techniques is a digital signature in combination with a public key infrastructure (PKI). This renders a verifiable digital certificate from a third party that authenticates each component to the other in an asymmetric encryption algorithm that is among the most secure, low-cost electronic technologies available. In the Diebold system, digital certificates exist at the server, but these are neither signed nor authenticated by the AccuVote terminals.

There should be some perspective on this vulnerability. It should be remembered that election night results are not official results and therefore have no legal importance. No one can assume office until the official election results are announced by the election officer. This occurs within 30 days of the election. Should there be an election night interception of results, there are typically enough controls in election procedures that would bring the deception to light within a day or so of the election. There would be ample time to check precinct results and determine the actual election outcome. This would certainly be an embarrassment to election officials and to the involved vendors, and it should be avoided, but it would likely not constitute a mechanism for “stealing an election.”

3.7.3 Recommendations

- 1) The State should require all voting system vendors operating in Arizona to implement two-way authentication between precinct and central count equipment for all transmissions, especially those of election night results.
- 2) The State should ensure that there are procedures for “double checking” transmitted election results for all elections in the State once materials are returned from the precincts.

¹ Authentication is substantiation that an entity is, in fact, who they claim to be.

² Raba Report, Page 9

3.8 Can Smart Card Fraud Occur With Diebold Products?

3.8.1 Description

Diebold technology uses a physical smart card that is inserted by the voter into the DRE system to display the relevant ballot. The card contains ballot information but not the vote of the voter¹. The card is given to the voter once the voter's registration is verified. The question is whether the voter could:

- 1) Vote more than once.
- 2) Bring in an additional (altered) smart card to the polling place and use it to load alternative instructions into the voting machine.

3.8.2 Analysis

Once given access to a smart card's contents, it is an easy matter to duplicate it, to change a voter card to a supervisor card (and vice versa) and to reinitialize a voter card so that it could be used to vote multiple times².

There is also a third type of card, the Security Key Card. This card allows election officials to change the default passwords used to secure the supervisor and voter cards. The process of changing these passwords is painless and takes approximately five seconds per AccuVote-TS terminal and Voter Card Encoder³.

Diebold has addressed many of the security issues raised by the independent reviews through the implementation of "umbrella" changes. In summary, below are some of the changes Diebold has implemented to their hardware, software and firmware:

- The supervisor card PIN is no longer hard coded as "1111".
- All data transmissions to, and from, the terminal are encrypted using SSL. The request was to encrypt the optional modem transmissions, but Diebold went ahead and used SSL for all communications including uploads and downloads taking place within secure rooms at election central.
- The DES encryption key used to encrypt election results is no longer hard coded.
- The smart card access key required to read from, or write to, the smart card is no longer hard coded.
- The election files on the PCMCIA card are now digitally signed such that any changes will be detected.
- Supervisor card PINs can now be up to 10 digits in length.

¹ Avante cards do record vote onto card

² Raba Report, Page 16

³ Raba Report, Page 17

3.8.3 Recommendations

- 1) If the State were to acquire AccuVote-TS terminals: It should:
 - a) Ensure that Security Key Cards are created with computer-generated passwords by precinct. It should also update all the Encoders and AccuVote-TS terminals within each precinct.
 - b) Apply Tamper Tape to AccuVote-TS terminals to prevent non-authorized entry of Security Key Cards into the terminals.
 - c) Institute strict procedures to prevent the use of unauthorized Supervisor Cards¹.

3.9 Does Diebold Have Adequate Internal Security?

3.9.1 Description

The question is: Do Diebold election systems lack adequate security mechanisms to protect internal company documents regarding its voting systems from outside hackers? For example, more than 13,000 internal Diebold e-mails and documents were taken from a Diebold staff server in March 2002 and delivered to voting activists and the media. In another incident, Diebold source code was posted to a publicly available File Transport Protocol (FTP) site. This code was downloaded and used by researchers at Johns Hopkins University to identify security flaws.

3.9.2 Analysis

Diebold claims that their software development environment is ISO 9000 compliant. This implies a degree of human and system security.

3.9.3 Recommendations

The State should encourage all election system vendors to conform to ISO 17799 security standards.² This will ensure that election system source code and documentation are not left at Internet-accessible FTP sites.

3.10 Did Diebold Disregard State-Certified Configurations?

3.10.1 Description

A State of California audit found Diebold in violation of the State's certification practices. The State revealed that the company installed uncertified software in all 17 counties that use its electronic voting equipment.

- 1) Fourteen (14) counties used software that had been qualified by federal authorities but not certified by State authorities.

¹ Raba Report, Page 17

² ISO17799 is "a comprehensive set of controls comprising best practices in information security". See: <http://www.iso-17799.com/>

- 2) Three (3) counties, including Los Angeles, used software that had never been certified by the State or qualified by federal authorities for use in any election. Action on the Diebold audit was pending as of 17 January 2004¹.

Arizona had a similar experience in which it was learned by the Secretary of State that versions of the Diebold software that were in use in Arizona counties had not been certified by the State.

3.10.2 Analysis²

There have been examples where Diebold has placed software upgrades or patches on machines without going through the certification process.

After a State of California investigation in November 2003, Diebold certification was made conditional. The audit discovered that the company had placed uncertified software on some touch-screen machines used in elections³. Subsequently, the State of California conducted a review of the March election and in particular, a review of Diebold equipment operation.

Following the March election experience⁴, the Secretary of State decertified the Diebold AccuVote TSx voting equipment for use in California and suspended the provision for six months notification, making its ruling effective immediately. In the SOS staff report⁵, it was noted that Diebold had not only disregarded the California State certification process, but had sold equipment and proceeded to implement equipment which had not been ITA certified (i.e., their newer DRE, the AccuVote-TSx).

Though Diebold has been in the news regarding this issue a great deal, many, if not most, of the other election system vendors have also been lax in strictly conforming to certified configurations. Further, states have been lax in requiring conformance to configurations. This has been an industry-wide issue and one by no means limited to Diebold.

3.10.3 Recommendations⁶

- 1) The State should hold Diebold (and all other election system vendors) to the recommendations in this report for Configuration Management.
- 2) The State should not acquire Diebold AccuVote TSx DREs from Diebold for voters with disabilities unless and until the certifications (both federal & state) have been resolved.
- 3) The State should consider an alternative DRE or another alternative solution for voters with disabilities.

¹ "E-Voting Undermined by Sloppiness" - <http://www.wired.com/news/evote/0,2645,61637,00.html>

² See Section on Configuration Management

³ Diebold Gets Stay in California, Wired News <http://www.wired.com/news/evote/0,2645,61947,00.html>

⁴ In April 2004

⁵ State of California Office of the Secretary of State Staff Report on the Investigation of Diebold Election Systems, inc., 20 April 2004

⁶ See Section on Configuration Management

3.11 Is Diebold An Objective Election Partner?

3.11.1 Description

There are, at minimum, three principle issues regarding the objectivity of Diebold as an elections partner:

- 1) *Statement Made by Diebold CEO* — Diebold President and CEO, Walden O'Dell, stated in a 14 August 2003 fund-raising letter to Ohio Republicans: "I am committed to helping Ohio deliver its electoral votes to the President next year." O'Dell has since stated that he regrets the wording in the letter: "I can see it now, but I never imagined that people could say that just because you've got a political favorite that you might commit this treasonous felony atrocity to change the outcome of an election."
- 2) *Sold Systems with Known Security Flaws* — Internal e-mails leaked to the media indicate that Diebold knew about security flaws long before it sold machines to several states, including California, Maryland and Georgia¹.

3.11.2 Analysis

The question is whether Diebold is objective as an election partner, not whether Diebold is the most competent, most secure, most well-managed election equipment vendor.

Walden O'Dell's comment was clearly made in the context of his political beliefs and not in terms of the operation of his election systems. It is clear that several executives at Diebold support their political beliefs through campaign contributions and such a practice, given the nature of their business, can be questioned on grounds of perception and prudence but not on grounds of legality or ethics. Recently, Diebold has banned campaign contributions by its executives².

It has been substantiated, however, that Diebold violated state certification laws on numerous occasions in order to ensure that elections conducted using their systems were successful. It should be remembered that until recently, strict adherence to certification configurations was not generally enforced by states regarding any election vendor's equipment.

Diebold has apparently sold systems that at least some of its staff knew had less than adequate security controls, but much of this occurred before the security of voting systems was challenged.

3.11.3 Recommendations

- 1) The State should closely monitor Diebold actions both within Arizona and around the country for compliance with security and certification requirements.
- 2) The State should closely monitor the financial health of Diebold's Elections Division.
- 3) The State should require a project plan from Diebold with financial penalties for not meeting milestones.

¹ "Diebold Backs Off Legal Challenge" -

[Http://www.wired.com/news/evote/0,2645,61243,00.html?tw=wn_polihead_1](http://www.wired.com/news/evote/0,2645,61243,00.html?tw=wn_polihead_1)

² "Diebold Bans Political Contributions", USA Today, 8 June 2004

- 4) The State should request regular periodic confidential briefings from Diebold executives on its steps toward correcting its deficiencies.

3.12 Recent Diebold Actions in Response to Critics

3.12.1 Some Perspective

Diebold is a firm with the largest market share in election equipment that in the past has failed to lead in product development and anticipation of market needs. Diebold, like most other election system vendors, failed to recognize the need to bring its products into compliance with modern security and certification requirements until issues were raised by others. Further, it should be noted that Diebold, and other election vendors, were not compelled to meet modern security standards by the national certification process. It has come to their attention, their competitors' attention and the attention of the public only by the activists and the leadership of some state election officials.

3.12.2 In Defense of Diebold Election Systems

Below is testimony from Diebold regarding the successful use of its election systems in the March 2004 Super Tuesday:

The numbers from the March Super Tuesday election tell a compelling story:

1. Zero security-related problems at the more than 55,000 Diebold touch-screen voting stations deployed across the country by elections officials
2. Over 9 million voters had the opportunity to use electronic voting solutions, including the entire State of Georgia and virtually the entire state of Maryland;
3. Almost 130,000 visually impaired men and women had an opportunity to vote without assistance;
4. 310,000 disabled people could vote more conveniently because the voting booth could accommodate them;
5. 61,000 new American citizens had the opportunity to vote on a ballot written in their native language;
6. 562,000 older Americans were able to vote easily and intuitively.

That's a proof of performance that is strong and irrefutable.¹

3.12.3 Response to Ohio Compuware Study

Diebold recognizes that it cannot ignore these issues and in recent months has moved aggressively to make corrections to its products and practices. In testimony in Ohio, Diebold reported the following regarding its response to the State of Ohio Compuware Report, November 2003:

There were a total of 18 recommendations relating to Diebold. Of those 18, only eight

¹ Testimony of Mark Radke, Director of Marketing, Diebold Election Systems before the Joint Committee on Ballot Security, 31 March 2004, Columbus, Ohio.

required changes in our system. The others were recommended procedural changes for election administrators. We were able to accomplish all of the system enhancements with four “umbrella” changes.

1. We removed all hard-coded encryption keys, passwords and PINs. All of these elements are now selected by each local board of elections and changed by them as often as they choose.
2. We encrypted and authenticated uploads of election results.
3. We have established a six-digit PIN for the supervisory functions.
4. We have digitally signed ballot definition files so that any unauthorized changes would be immediately detected.

Again, Diebold Election Systems has already made every single one of the recommended changes in our system and has submitted those changes for review by the independent testing agencies [ITAs]. In fact, those changes were reported by the Secretary of State on February 26th. I would note for the record that Diebold was the first company to comply with these changes and that we were able to do so at least 45 days ahead of our competitors.¹

3.12.4 Response to the RABA Study

Diebold made a key point regarding much of the issues regarding voting system security in its response to the RABA Study. The point is that voting system security is a combination of technical security features and election procedures. Further, many of the apparently technical vulnerabilities of election systems have, and continue to be overcome by, election procedures that ensure that many theoretical vulnerabilities are not realistic vulnerabilities. Again, Diebold testimony in Ohio:

In fact, one of the leading critics acknowledged that fact after he served as a poll worker in the March Primary. Professor Avi Rubin wrote the following: "In our paper, we described how the smartcards used by these machines had no cryptography on them, and we made the widely criticized claim that a teenager in a garage could manufacture smartcards and use them to vote 20 times. I now believe that this particular attack is not a real threat." Later in his recounting of his Election Day experience he said, "I started realizing that some of the attacks described in our initial paper were actually quite unrealistic, at least in a precinct with judges who worked as hard as ours did and who were as vigilant." He also said this: "One thing absolutely amazed me. With very few exceptions, the voters really LOVED the [DRE] machines. They raved about them to us judges. The most common comment was 'That was so easy.'" Now, I'm not suggesting that Professor Rubin has converted. In fact, he continues to object to electronic voting, but it is instructive that his eyes were opened to some of the checks and balances of our overall voting system.²

¹ Testimony of Mark Radke, Director of Marketing, Diebold Election Systems before the Joint Committee on Ballot Security, 31 March 2004, Columbus, Ohio.

² Testimony of Mark Radke, Director of Marketing, Diebold Election Systems before the Joint Committee on Ballot Security, 31 March 2004, Columbus, Ohio.

3.12.5 Diebold Announces Restructuring of Compliance and Certification Processes

In December 2003, Diebold (DESI) announced the following changes to its compliance and certification processes with the intention to rectify past issues regarding certification compliance:

Creating Compliance and Certification Officer Position

DESI is reorganizing how it administers qualification and certification processes internally. A new department, headed by a Compliance and Certification Officer, will have oversight for all compliance and certification responsibilities. In the past, these responsibilities were managed on a regional basis because of the geographical diversity of our customer base.

Immediate Compliance Review of all Software, Firmware and Hardware

DESI has instituted a thorough internal compliance review of all hardware, firmware and software across its customer network covering more than 30 states. The Compliance and Certification Officer has direct oversight responsibility for the review.

Formalize Compliance and Certification Process

All issues concerning qualification and certification compliance will be administered by the Compliance and Certification office. DESI has implemented stringent internal controls and procedures that formalize the compliance processes it employs with the respective governing and certification authorities and its customers. This will include specific procedures to manage requests for upgrades from customers.

Clarifying Notification and Certification Requirements with Customers and States

DESI is drafting new provisions for all current and future contracts that will specifically delineate duties and responsibilities related to notification, qualification and certification requirements for upgrades, product changes, etc. These provisions will apply to all upgrades whether required by state law or regulation, or requested by one of its customers.

"Our intent in making these organizational changes is to ensure the public's confidence that all of our hardware, software and firmware products are fully certified and qualified by all of the appropriate federal, state and local authorities prior to use in any election," said Urosevich. "Helping ensure the right for all to vote reliably, privately and accurately, including the sight disabled, is of paramount importance to us. Electronic voting makes that possible, and we will continue to improve our processes and technology as we move forward."¹

¹ "Diebold Election Systems Announces Restructuring of Compliance and Certification Processes", Diebold Press Release, December 2003.

3.12.6 Future of Diebold As Election Vendor

It should be noted that election systems represent only about five percent of Diebold's overall business. Diebold's financial health is very closely tied to the financial market place as a large portion of its business involves that sector of the economy. A downturn there could affect Diebold's ability to support its election business. Conversely, Diebold could decide and easily accomplish an exit from the elections business, perhaps concerned that negative press may hurt its core business. Though this issue has been raised among Diebold investors, Diebold recently declared that it will remain in the election system business¹.

¹ "Diebold's Voting Machine Expansion Rattles Investors and States", Bloomberg News, 21 May 2004

4.0 Questions Regarding Voting in Arizona

4.1 Has Arizona Acquired Diebold Voting Systems That Are HAVA Compliant?

4.1.1 Description

The State of Arizona recently acquired new Diebold optical scan (not DRE) voting systems to replace punch card systems deployed in nine (9) Arizona counties. The State entered into a contract with Diebold to supply the optical scan equipment to the counties who would then purchase the equipment from Diebold using both Federal HAVA grants and county funds. Currently all nine (9) counties have replaced their punch card systems with Diebold's optical scan systems and have used them successfully in one statewide and two local elections.

Federal HAVA legislation mandates that DRE or other accessible voting devices be used for voters with disabilities. The State of Arizona is currently in the process of determining which voting devices would meet this requirement. Although the State of Arizona had not recommended a specific DRE solution, Yavapai County has purchased and used Diebold DRE voting equipment on a limited basis, both for early voting and for use by voters with disabilities.

4.1.1.1 RFP & Selection

The State of Arizona issued a Request for Proposal (RFP) for election optical scan technology systems in August 2003. Three vendors responded:

- 1) Diebold
- 2) ES&S
- 3) Avante

The State selected Diebold Optical Scan Equipment as the standard for the Arizona counties who were required to replace their punch card systems. The State determined that it would purchase Direct Recording Electronic (DRE) systems (i.e., touch screen voting devices) on a limited basis for use by voters with disabilities, in accordance with HAVA requirements that the right to cast a secret ballot be extended to voters with disability by 2006.

4.1.1.2 Award

Accordingly, the State awarded a contract to Diebold for 440 optical scan voting machines at a cost of \$3–\$5 million. The contract included the cost of the equipment, service and support for the nine (9) counties that will be implementing the new voting technology.

4.1.1.3 Funding

Arizona is slated to receive \$27 million in HAVA federal funds in FY2004. Of this amount, the State has thus far received \$7 million for which the State was required to provide a five percent match. The match was appropriated in the State Budget at \$800,000 for FY2004 and \$1.4 million for FY 2005 so far. Arizona expects to receive \$40 million over a three-year period.

- 1) Year 1: Received \$7 million in HAVA funds and the State matched \$800,000.
- 2) Year 2: Expect to receive \$27 million and with a state match of \$1.4 million¹.

The Diebold systems were purchased with HAVA Title I funds while the new statewide voter registration system will be funded with HAVA Title III funds.

Other remaining HAVA funds will be used to buy voting devices for voters with disabilities and to train poll workers.

4.1.1.4 County Implementations

The State has a Memorandum of Understanding (MOU) regarding how the nine (9) counties will pay for the systems that replaced their punch card systems and for how they will be implemented. If the counties want to take advantage of available HAVA funds, then they must buy through the State contract with Diebold. If counties have their own funds, then they can purchase any voting equipment, including DREs, so long as they have been certified by the State.

4.1.1.5 Election Results

All nine (9) counties implemented new technology that was used in the 3 February 2004 Presidential Preference Election. Those elections proceeded without any major problems. The only issues that arose were:

- 1) *Reliance on Diebold* — Reliance on Diebold staff was required to run the machines because there was not enough time to train county staff.
- 2) *Snowstorm* — A snowstorm occurred that slowed the transport of some results.

The Secretary of State's office asked the (9) counties and Diebold to submit reports on "Lessons Learned." The State met with the (9) counties the first week of April 2004 and discussed the election process and "lessons learned." As documented in a letter² to Diebold, the "lessons learned" were the following:

4.1.1.5.1 Hardware

- 1) *Memory Cards* — All nine counties had a significant number of memory card failures. Mojave County had a memory card failure rate of approximately 25 percent. Diebold acknowledged that this failure rate was unacceptable. They are currently working with the manufacturer of the cards to determine the source of the problem. They anticipated that the evaluation would take until early to mid June. At that point, a decision will be made whether or not only the troubled cards should be replaced or all memory cards should be replaced. This issue is to be resolved prior to the fall elections.
- 2) *Ballot Boxes* — Many counties had troubles with their ballot boxes not working properly. The ballot boxes did not align properly with the voting systems, causing ballot-feeding problems.

¹ The matching amount is for the whole project and each individual match may not exactly correlate with the federal amount since two separate government agencies appropriate the monies.

² Letter from Kevin Tyne to Mr. Barry Herron, Vice President of Sales, Diebold Election Systems, dated 20 April 2004.

The ballot boxes are made of plastic so factors such as temperature can cause slight modifications to the ballot box form. Diebold has been working with some counties to adjust the ballot boxes to resolve the problem. Diebold has indicated that the ballot boxes will be either adjusted to fix the problem or replaced outright if adjustments do not resolve the problem.

4.1.1.5.2 Software

- 1) *GEMS* — The GEMS version used by all nine counties did not generate a Statement of Votes Cast (SOVC) properly. A prior version of GEMS needed to be loaded in order to generate this report. As this report is a standard and essential component of any GEMS version, county staff were dismayed and disappointed that Diebold had not provided them with the certified version of GEMS. This SOVC report issue has been addressed in the next version of GEMS, version 1.18.19. The testing by the ITA was completed on 20 April 2004, and 1.18.19 was federally certified in the summer of 2004.
- 2) *Software Glitches* — Arizona expressed concern regarding the issues that were raised in the Oakland Tribune Article titled "E-voting probe finds no reason for glitches" dated 13 April 2004. Since the article mentioned issues Alameda County had with the same version of GEMS as used by Arizona, an explanation of the findings and proposed solutions to fix the software was requested of Diebold.

4.1.1.5.3 Support

- 1) *GEMS Training* — Some counties had no, or limited, GEMS training. Diebold's implementation plan was to first train the counties on the equipment and then train the counties on GEMS. It was deliberate to use the PPE, the March and the May elections to get the counties very familiar with the equipment and then use the summer to train on GEMS. The GEMS training was scheduled for 14–18 June.
- 2) *Inconsistent Support Personnel* — Some counties complained that the Diebold support personnel they had assigned to them would change without much notice. These counties expressed a desire to have consistent support personnel assigned to them through the entire election process. Diebold has a support structure that allows any support person to address an issue at any county. Diebold feels that this is the best approach since it allows for the quickest response to problems and reduces the dependency on any one person. SOS emphasized to Diebold that the communication of the support approach needs to be clearer and that counties should know what to expect for each election from a support perspective.
- 3) *Inexperienced Support Personnel* — Some counties complained that the technical troubleshooting support personnel assigned to their county had virtually no training or experience with Diebold equipment prior to showing up at the county. Diebold is revamping its employee training approach and developing a national training practice. The training for new personnel will be more comprehensive and consistent. Diebold promises to address any support deficiencies that are brought to its attention.

4.1.2 Analysis

4.1.2.1 Use of Optical Scan Equipment

Optical scan systems include an artifact, the scanned paper ballot that remains after an election is held and can be used to conduct a recount. Thus, the paper ballots can be used to ensure that the votes cast are the votes counted, and can be easily voter-verified before deposit in the ballot box. This technology also does not involve the security concerns of DRE technology regarding the use (and misuse) of software and smart cards.

Some Advantages of Optical Scan Voting	Some Disadvantages of Optical Scan Voting
Provides an artifact of votes cast that can be used to perform a recount.	There is limited space in which to place contest choices
Easy for voters to understand voting method	Vote counting is not as fast as DRE
Cheap and easy to accommodate increased volume of voters by adding additional non-mechanical voting booths at the precinct.	Paper and printing are expensive (and sometimes wasteful)

4.1.2.2 Use of DRE Systems for Disabled Voters

Arizona must comply with HAVA requirements mandating the use of a voting device that ensures a secret ballot for disabled voters by 2006. Arizona is in the enviable position of not having committed yet to a specific solution or vendor for this purpose. The State thus has the opportunity to ensure that it selects a solution that meets HAVA requirements and avoids issues that have been raised about security, reliability, recount capability and voter verification.

4.1.2.3 Use of Central Count Equipment

One of the vulnerabilities of optical scan systems that are shared with DRE systems is the security of the central election management system. The Diebold system uses its GEMS software while the ES&S system uses its UNITY software. The security issues have been outlined in the analysis of Diebold DRE systems above, and are summarized as follows:

- 1) Inadequate access password protection of central count databases
- 2) Inadequate authentication and encryption of data as it is transmitted from precincts via modem over telephone lines to central county tabulators
- 3) Insufficient rigor regarding software development
- 4) Inattention to conformance with certified version control

4.1.2.4 Conclusions

Arizona is in an enviable position relative to many states. It has moved forward with elimination of punch card systems, but has done so without significant investment in the controversial DRE technology. It is positioned to meet HAVA disability requirements and can do so with the benefit of improved solutions to be offered by vendors now that the public is aware of the issues regarding DRE solutions.

4.1.3 Recommendations

- 1) The State should continue to use and deploy optical scan voting technology as its standard now and into the foreseeable future.
- 2) The State should continue to actively seek and deploy technology advances in optical scan systems to further enhance their efficiency and effectiveness.
- 3) The State should publicize its commitment to optical scan technology and educate voters that most of the controversy surrounds DRE technology that is used by less than one percent of the voters of the State.
- 4) The State should ensure that any statewide solution chosen for compliance with HAVA regarding secret ballots for disabled voters minimizes concerns regarding the security, reliability and voter verification issues of current product DREs.
- 5) The State should consider alternative technologies that operate like DREs but record on scannable paper documents.
- 6) The State should continue to work with disability groups to ensure that an optimal solution that will meet their needs is deployed.

4.2 Does Arizona Have An Adequate Voting Certification Process?

4.2.1 Description

4.2.1.1 History of Voting Certification

The availability of relatively cheap computers coupled with advances in punch card technology and optical scan technology in the mid-1970s led to a new cottage industry in voting equipment. With no federal guidelines and little state supervision, election officials had to work the anecdotal evidence and vendors' recommendations to select election systems.

In 1975, the General Accounting Office's Office of Federal Elections¹ and the National Bureau of Standards² released a report that concluded:

One of the basic causes for computer-related election problems was the lack of appropriate technical skills at the State and local level for developing or implementing written standards, against which voting system hardware and software could be evaluated.³

Based on the report and follow-up testimony from local election officials, Congress commissioned a study on the feasibility of developing voluntary standards for developing and using voting systems in the United States. This effort culminated in the 1984 report, "Voting System Standards: A Report on the Feasibility of Developing Voluntary Standards for Voting Equipment."

¹ GAO Office of Federal Elections was the predecessor to the Federal Election Commission (FEC).

² The NBS was the predecessor of the National Institute of Standards and Technology (NIST).

³ "Effective Use of Computing Technology in Vote-Tallying", GAO Office of Federal Elections, 1975.

Congress then appropriated funds for the FEC to develop standards. The Commission completed the task and the first standards were approved in January 1990. NASED developed procedures to validate equipment against the standards, and certified a small number of ITAs to actually test the equipment. By 2001, 37 states had adopted the voluntary standards.

After the 2000 presidential elections, three significant developments further affected voting system standards.

- 1) The FEC updated the voluntary standards in 2002.
- 2) The Election Assistance Commission (EAC) was established by Congress as part of the Martin Luther King Help America Vote Act of 2002, finally being introduced as a body in February 2004. HAVA also directly outlawed certain voting machines for use in federal elections, and allocated funds to replace old voting equipment.
- 3) HAVA also calls for cooperation between the EAC, NIST and the Technical Guidelines Development Committee in refining voting standards.

4.2.1.2 Current Arizona Certification Process

In the absence of strong guidance from the federal governments, many states continued from the 1990 guidelines or developed other guidelines. Arizona determined that the Secretary of State shall be responsible for approving electronic voting equipment, and for establishing practices to run elections, tally results, and handle ballots.

4.2.1.3 Current Arizona Voting System Requirements

The Arizona Revised Statute, Title 16, Chapter 4, §16-446 details the specific requirements for electronic voting machines. The requirements list is relatively brief. Here is the text of §16-446 Specifications of electronic voting systems:

- A. An electronic voting system consisting of a voting or marking device in combination with vote tabulating equipment shall provide facilities for voting for candidates at both primary and general elections.
- B. An electronic voting system shall:
 1. Provide for voting in secrecy when used with voting booths.
 2. Permit each elector to vote at any election for any person for any office whether or not nominated as a candidate, to vote for as many persons for an office as he is entitled to vote for, to vote for or against any question upon which he is entitled to vote, and the vote tabulating equipment shall reject choices recorded on his ballot card or paper ballot if the number of choices exceeds the number which he is entitled to vote for the office or on the measure.
 3. Prevent the elector from voting for the same person more than once for the same office.
 4. Be suitably designed for the purpose used, of durable construction, and may be used safely, efficiently and accurately in the conduct of elections and counting ballots.

5. Be provided with means for sealing the voting or marking device against any further voting after the close of the polls and the last voter has voted.
6. When properly operated, record correctly and count accurately every vote cast.

Elsewhere in the statutes are provisions for the specific Arizona-Wyoming Ballot Rotation and other general requirements for voting equipment.

The Secretary of State creates and maintains “The Official Instructions and Procedures Manual.” The manual is published after consultation with county elections officers. After approval by the Governor and the Attorney General and pre-clearance by the U.S. Department of Justice (DOJ), it has the force of law and there are specific penalties for non-compliance. Arizona Revised Statute now requires full testing and certification by a federally accredited laboratory pursuant to HAVA.

4.2.1.4 Certification and De-Certification

Power to Certify — In accordance with Arizona Revised Statutes §§ 16-441 and 16-442, the SOS appoints a three-member committee¹ to review election equipment and make a recommendation to the SOS regarding approval for use in State and local elections. The membership of the committee is designated as follows:

- 1) One member must be from the engineering schools of one of the State universities.
- 2) One member must be from the State Bar of Arizona.
- 3) One member must be knowledgeable about voting in Arizona.

No more than two members can have the same political party affiliation.

While the law provides that the panel shall test the various machines, it does not prescribe the manner in which the machines shall be tested.

Power to De-Certify — The SOS has the authority to decertify equipment as per ARS 16-442(C).

4.2.1.5 Application Requirements

Applications for certification must include the ITA reports and results, the NASED numbers and any materials describing and documenting the product.

4.2.1.6 Test Demonstration

The State requires a test demonstration of vote recording or tabulating machines or devices proposed for State approval. The test demonstration must demonstrate that the system can provide for²:

- 1) An open or closed primary system
- 2) Candidate name rotation using the Arizona/Wyoming method¹

¹ The Certification Committee

² For more detailed certification requirements, see Arizona Revised Statutes, Title 16, Chapter 4 — Article 3; Article 4; Article 5; Article 6; Article 10 and Article 11. The link to these statutes is <http://www.azleg.state.az.us/ArizonaRevisedStatutes.asp>.

3) Cumulative tabulation by office, by precinct and by county

4.2.1.7 Emergency Certification

As part of the existing certification process, SOS provided emergency certification for counties that had been using equipment that had not been certified. This emergency certification was done in view of the hardship that would be placed on counties if they were required to change to the then certified equipment. The State has provided emergency certification in one instance to provide relief to Pima County to enable it to operate its elections.

4.2.2 Analysis

4.2.2.1 Criteria for Selection

To determine best practices in certification processes, a set of criteria were established for the review of certification processes in other states. The criteria that were established are as follows:

- 1) **Budget and Population** — The state is similar in population size and budget to Arizona.
- 2) **Recently Certified At Least One System** — The state has evaluated at least one system since 2000.
- 3) **No Successful Challenge** — The state has not had a successful challenge to a rejected system since 2000.
- 4) **Not Totally Reliant on ITA or Other State** — The state certification process does not rely solely on ITA certification or certification in another state, but actively conducts its own certification process.
- 5) **Well Documented** — The state has a certification process that is well documented.
- 6) **Recognized in Literature** — The state has been recognized in the literature as having a quality certification process.

4.2.2.2 Best Practices in Other States

Many of the 37 states that have adopted the federal voluntary standards, such as Alaska and Washington, rely solely on ITA certification. Others, such as Iowa, have undocumented certification criteria. Georgia and Delaware have adopted uniform voting systems across their respective counties. Alabama requires vendors to self-certify that they meet the state's requirements, but does not perform its own certification process.

¹ see A.R.S. §§ 16-462 through 16-468, 16-502 and 16-506(C)

Table 1. High-Level Comparison of State Election System Certification Processes

Criteria	California	Louisiana	Alaska	Idaho	Iowa	Montana	North Dakota	Texas	Utah	Washington
1. Budget & Population — The state is similar in population size and budget to Arizona.		X								X
2. Recently Certified At Least One System — The state has evaluated at least one system since 2000.	X	X		X	X	X	X	X	X	X
3. No Successful Challenge — The state has not had a successful challenge to a rejected system since 2000.	X	X		X	X	X	X	X	X	X
4. Not Totally Reliant on ITA or Other State — The state certification process does not rely solely on ITA certification or certification in another state, but actively conducts its own certification process.	X	X		X		X	X			
5. Well Documented — The state has a certification process that is well documented.	X		X	X		X	X	X	X	X
6. Recognized in Literature — The state has been recognized in the literature as having quality certification process.	X									
Total	5	4	1	4	2	4	4	3	3	4

Though there were other states that matched “Xs” with Louisiana regarding our criteria, the criteria of similar size and budget was an overriding consideration when comparing these states. Louisiana, among the states that were “tied,” is the most similar in terms of size and budget to Arizona. Consequently, Louisiana was selected (along with California) as a best practice state of interest to Arizona.

4.2.2.3 California

California is the state with the largest voting population. The California Secretary of State has similar responsibilities and authorities in California to those of the SOS of Arizona regarding voting system regulations.

After the 2000 elections, Judge Stephen V. Wilson ruled in *Common Cause v. [Secretary of State Bob] Jones* that the Votematic and Pollstar punch card machines used in nine (9) California

counties had disenfranchised thousands of California voters and needed to be removed from service before the 2004 presidential election.

Secretary Jones' successor, Secretary of State Kevin Shelley, recently used the powers of his office to decertify specific models of electronic voting machines. California has a well-designed and well-documented process for certification and de-certification of voting systems.

California documents the actual certification process, the formation of the committee, and the steps that the state takes during the process. The best information from California is about process¹.

4.2.2.4 Louisiana

After surveying the states, Louisiana was judged the most acceptable match. The state's 2.8 million registered voters compare well with Arizona's. Also, Louisiana's state budget of \$6.7 billion is comparable to Arizona. Louisiana states it has had eight (8) applications and certified four of them since 2000.

In 1999, Louisiana's *ex-officio* Commissioner of Elections Jerry Fowler pled guilty to State and Federal charges after a scandal concerning a bribe of \$8 million from Sequoia to purchase its voting system for the state. Louisiana reformed its certification and procurement practices under the guidance of new Commissioner of Elections Suzanne Haik-Terrell, the state's first woman to hold the office. During Commissioner Terrell's tenure, the legislature passed Act 451, a sweeping reform act that placed the responsibility for managing the election process back with the Secretary of State's office.

The Louisiana documents focus on the election systems criteria, including how the systems must perform, what the electrical characteristics are, and what conditions must be acceptable during storage and shipping. The best information from Louisiana is about functionality.

4.2.2.5 Desired Guidelines for Certification

Desired Guideline	Included in Best Practice Guideline
Guidelines for certification of functionality	Yes
Guidelines for certification for security	Yes
Guidelines for certification for major and minor software upgrades and other technology changes	Yes
Guidelines for emergency certification process	Yes
Guidelines for examination of voting system source code	Yes

¹ See California certification process in "Appendix D — State of California Certification Procedures."

4.2.3 Recommendations

- 1) The State should revise its Certification Process in accordance with the Best Practices Certification Process developed in this report (See Appendix B — Best Practice Certification Procedures).
- 2) The State should review current Arizona Election Law to ensure that it has the capability to grant emergency conditional certification to voting systems that have been ITA approved, but which need an upgrade that is not yet ITA certified though necessary, in the judgment of the SOS, to conduct state or local elections in Arizona.

4.3 Does Arizona Have Sufficient Procedures to Ensure That Configuration Certified is Configuration Used?

4.3.1 Description

In Arizona, as in most states, the certification procedures have not been specific in the past as to the exact level of system configuration that was certified. Recently, the State required specific certification by software version number as defined by the vendor of the equipment and software. The current list of certified equipment has certification at varying degrees of configuration, e.g., some by version number and some not. A determination needs to be made as to what constitutes a complete definition of a system and how once certified, that definition can be verified as that which is in use.

An example of this configuration certification issue occurred in California, where an audit uncovered discrepancies between what was certified by the State and what was actually in use in various counties. At least five counties were using versions of software or firmware that were different from that which had been certified. The most serious issues related to the Diebold GEMS central count tabulation software.

Although the last version of GEMS certified in California was 1.17.17, auditors found that no county was using it. Instead, they were using more recent versions such as 1.17.20, 1.17.23 and 1.18.18.102. Versions 1.17.20 and 1.18.18.102, however, were never certified by federal-level ITAs.

4.3.2 Analysis

This issue arises because election equipment in the past was relatively simple such that a model number was sufficient to define fully that which was certified. Today, incremental modifications are made to software, firmware and even hardware such that many more specifications are required to define fully that which is certified. Many states have been caught unaware in this transition.

Configuration management is the process of managing the set of component versions that fully define a particular configuration of a system. It is a discipline (with attendant software tools) that has been developed in the IT industry to address the issue of adequately managing the advance (and retreat) of operational systems toward newer versions. Typically, the set of component versions that are in operation is noted as the current “build.” A set of component versions is assembled, including new versions of some components, denoted as a new “build” and tested as a complete system. After satisfactory testing, the new build is swapped in for the current build and

thus a new (and improved) version of the product is put into production. Rarely, but on occasion, problems are encountered with the new “build” and a return to the previous build is required. The Configuration Management process indicates the exact set of versions that was in production previously, and that “build” is returned to production until problems with the new “build” can be resolved.

Like other IT system vendors, voting system vendors continuously update the configuration of their software and system components in order to improve the product and meet any additional customer requirements.

Until recently, Arizona had been certifying election systems by model or brand and not by version of components. Now certifications are conducted by principal software version number. However, the definition of what constitutes a version change is not standard and depends on the vendor. Some may argue that security patches and software bug fixes may be applied to the system but may not be considered a software upgrade and hence the version number would not be changed. Under this scenario, it is possible for significant changes to be made to a system without altering the principal software version number.

Poor configuration management is a potential vulnerability in election system management, as lack of it, on the part of the State, can result in the placement of all trust in the good faith and competency of the vendor. For Arizona there has not yet been a significant issue regarding software configuration. Without modification of its procedures, however, the State will be vulnerable to problems in the future.

4.3.3 Recommendations

- 1) The State should lobby ITAs to require all election system vendors to submit their products in “builds” for federal-level certification.
- 2) The State should lobby ITAs to test the specific build submitted and certify it. ITA certification should be accompanied with the exact version numbers of every hardware, software and firmware component of the system.
- 3) The State should test and certify the specific build of a system that was certified by an ITA.
- 4) The ITAs and the State should require re-testing and re-certification for any modification to the certified build, including “bug fixes” or “security patches.”
- 5) The State should communicate this requirement to all vendors supplying Arizona with election systems.
- 6) The State should develop a consistent process in conjunction with each county that would monitor all activities that involve changes or fixes to software and system components.
- 7) The State should develop a simple automated tool that can be used by all counties that would log all such activity.
- 8) The State should require vendors to provide a complete list of component versions contained within each release (build) and explain changes.

- 9) Vendors should provide releases (builds) that are digitally signed, and ITA should also digitally sign the release to provide assurance that election officials are in receipt of the certified version.

4.4 Does Arizona Have Adequate Voting Physical Security?

4.4.1 Does Arizona Have Adequate Physical Security in Storage of Equipment and Ballots?

4.4.1.1 Description

Since counties vary in size, resources and facilities, there is no common standard for the physical security of ballots and equipment across the State. Counties differ in the degree of physical security they maintain for voting equipment and ballots.

4.4.1.2 Analysis

Each county in Arizona is responsible for storing voting equipment and ballots and each county has its own practices of handling and storing equipment just before an election is held. For example, some counties allow precinct inspectors to keep voting equipment at their private residences the night before an election while others do not. These practices reflect the unique logistical challenges that each county and precinct faces.

The Secretary of State has not developed statewide guidelines regarding the specifics of storing voting equipment and ballots. While Gartner observed common sense practices in six (6) counties to ensure physical security, these are not consistent. All counties seal voting equipment with tamper-proof seals before they are deployed, so regardless of whether they are stored in a residence or at the precinct, any security breaches can be detected. It would be unreasonable to expect the same exact procedure to be undertaken by both Maricopa County and by Santa Cruz County. Some minimal guiding principles would help ensure that egregious oversights do not occur.

Nearly all of the six (6) counties Gartner visited complained that State statutes require that they store cast ballots for 24 months following the election. This requires significant storage and would appear to serve no real purpose since elections are declared by the SOS within 30 days following Election Day.

4.4.1.3 Recommendations

- 1) The State should emphasize (perhaps in Statute) that counties are responsible for the physical security of voting equipment and ballots.
- 2) The State should develop minimally acceptable guiding principles for the physical storage of voting equipment and ballots. For example, a minimal guiding principle might be to check and record tamper-proof seals as they leave the warehouse and again just before they are deployed at the polling place to ensure that no changes have occurred.
- 3) The State should revise the requirement for the storage of ballots for 24 months following an election, to a much-shorter duration.

4.4.2 Does Arizona Have Adequate Physical Security in Transport of Equipment and Ballots?

4.4.2.1 Description

The process of physical transport of voting equipment and ballots varies across the State and may not be secure in all counties.

Some counties rely on their own staff and resources to conduct physical transportation, while others hire temporary workers and vehicles for transportation. There is no defined standard for the physical transport of voting equipment and ballots.

4.4.2.2 Analysis

In our review of six counties, it was clear that each piece of vote recording and counting equipment is sealed individually to avoid any tampering.

4.4.2.3 Recommendations

The State should consider, in consultation with the counties, development of minimum election equipment transport physical security requirements.

4.4.3 Does Arizona Have Adequate Physical Security at Polling Places?

4.4.3.1 Description

Arizona counties may not have adequate or uniform physical security in all polling places.

4.4.3.2 Analysis

Determination of the physical security of polling places is done at the county level. There does not appear to be a defined standard for the physical security of the polling places. There has also been no reported threat of disruption, theft, alteration, sabotage or intimidation at polling places in Arizona. Still, in light of increased awareness of terrorism especially associated with elections and election results, it would appear prudent to examine what might be done to increase the security of vote casting, storage and transport.

4.4.3.3 Recommendations

The State should consider, in consultation with the counties, development of minimum polling place physical security requirements.

4.5 Does Arizona Have Adequate Poll Worker Training?

4.5.1 Description

With the introduction of relatively complicated electronic equipment, election administrators and poll workers need a higher level of training to operate elections using these technologies than was required with punch card systems.

Arizona counties conduct their own elections and generally do not rely on the vendor to provide onsite support for equipment. With the introduction of some DRE machines, there may be a

concern that current poll workers will not have adequate training to effectively operate the machines and resolve any technical issues that may arise.

4.5.2 Analysis

4.5.2.1 *Ballot Design and Printing*

Many counties¹ contract to the same vendor² to design and test ballots, program memory cards and coordinate ballot printing. Some counties have no in-house expertise for these functions. The use of a single vendor statewide for these services represents a potential single point of failure (SPOF) for many local, state and national elections in Arizona. Though the vendor has rendered excellent service to the counties, there remains the possibility that at some point in the future, this vendor may not be able to perform these functions. Should that occur, these counties will be “scrambling” to find resources and would likely turn to the equipment vendor who is not familiar with the specific ballot requirements of Arizona and of each county. This could lead to delays and unanticipated expenses for these counties.

4.5.2.2 *Poll Worker Training*

With adequate training, poll workers (of any age) generally have the ability to perform their duties effectively using optical scan and DRE voting technologies. Arizona has not encountered any major issues regarding poll worker training. Current county training procedures appear adequate to Arizona’s needs. The State has developed a standard election manual and most counties have developed supplementary poll worker procedure manuals and help guides. The use of optical scan equipment is now standard across the State, enabling greater collaboration among the counties toward improved procedures, guides and training techniques.

If DRE systems are deployed in limited quantities throughout the State to address disabled voter and voter verification issues, additional and different election administrator and poll worker training will be required.

4.5.3 Recommendations

- 1) The State Elections Manual is an achievement that has been beneficial to all the counties and citizens of the State. The State should ensure that there are adequate resources to ensure that the manual is maintained and enhanced into the future.
- 2) The State should monitor this skill set and ensure that it is covered for each type of equipment in use in the State.
- 3) The State should monitor poll worker training and foster opportunities for counties to share “lessons learned” with their peers.

¹ Including Graham, Cochise, Pima and Apache

² Election Operations Services, Inc.

5.0 Review of Selected Arizona County Election Systems and Processes

5.1 Description

Gartner reviewed the election systems and processes of the six Arizona counties that were not involved in the recent statewide procurement and upgrade of voting systems from older punch card technology to Diebold optical scan systems. These counties had previously moved away from punch card technology and were already using Diebold or ES&S vendor provided systems. The six counties analyzed were:

- 1) Apache County
- 2) Pima County
- 3) Yavapai County
- 4) Maricopa County
- 5) Cochise County
- 6) Graham County

The Table below shows a summary of basic voting statistics for the selected counties while the subsequent table indicates the voting technology used by each of the selected counties. Note that Maricopa County represents 60 percent of the population of Arizona and that Apache County has the highest rate of voting participation among the selected counties.

Table 2. County Demographics (March 2004)

County	% of State Population (1990)	Population (2004) Estimate	Percent of State Population (2004)	Voter Registration March 2004	Voters as Percent of Population	Percent of State Registered Voters	Number of Precincts March 2004	Average Voters per Precinct
State	100%	5,130,632	100%	2,274,367	44%	100%	2,108	1,078
Apache	1%	69,423	1%	39,083	56%	2%	45	869
Pima	16%	843,746	16%	385,917	46%	17%	401	962
Yavapai	3%	167,517	3%	83,983	50%	4%	103	815
Maricopa	62%	3,072,149	60%	1,329,076	43%	58%	1,058	1,256
Cochise	2%	117,755	2%	51,414	44%	2%	64	803
Graham	1%	33,489	1%	14,678	44%	1%	18	815

Table 3. Elections Technology

County	Provider	Voting	Central Count	Ballot & Reporting
Apache	Diebold	AccuVote Optical Scan (OS) V 1.94	AccuVote Tabulator	1) AccuVote ES 2000 Firmware 1.94w 2) Global Election

				Management System (GEMS) V1.18.18
Pima	Diebold	AccuVote Optical Scan (OS) V-1.94	1) AccuVote Tabulator 2) Central Count Diebold Feeders V 2.0.10	1) AccuVote ES 2000 Firmware 1.94w 2) Global Election Management System (GEMS) V1.18.19
Yavapai	Diebold	1) AccuVote Optical Scan (OS) 2) AccuVote TS (10) DREs for early voting. Use Optical scan for absentee voting	Do not have central count	1) AccuVote ES 2000 Firmware 1.94w 2) Global Election Management System (GEMS) V1.18.18
Maricopa	ES&S	Optech III-P (Eagle)	ES&S Optech Model IV-C	ES&S Unity V- 2.2 ETP Version 1.06AB
Cochise	ES&S	ES&S Model 100	ES&S Model 150 (Central Count) 150 ballots/min.	ES&S Unity Version 1.0 (ERS 6.3.10)
Graham	ES&S	ES&S Model 100	Do not have central count	ES&S Unity Version 1.0 (ERS 6.3.20)

5.1.1 Apache County

5.1.1.1 County Demographics

County	% of State Population (1990)	Population (2004) Estimate	Percent of State Population (2004)	Voter Registration March 2004	Voters as Percent of Population	Percent of State Registered Voters	Number of Precincts March 2004	Average Voters per Precinct
State	100%	5,130,632	100%	2,274,367	44%	100%	2,108	1,078
Apache	1%	69,423	1%	39,083	56%	2%	45	869

Apache County is approximately 70 percent of the Navajo Nation with 33 of its 45 voting precincts located in the Navajo Nation. The population is largely rural and mostly Native American.

5.1.1.2 Elections Technology

County	Provider	Voting	Central Count	Ballot & Reporting
Apache	Diebold	AccuVote Optical Scan (OS) V 19.4	AccuVote Tabulator	3) AccuVote ES 2000 Firmware 1.94w 4) Global Election Management System (GEMS) V1.18.18

5.1.1.3 Elections Organization and Staffing

In Apache County, elections are run by the Clerk of the Board of Supervisors, while voter registration and early voting are the responsibility of the County Recorder. The County registration roll is verified against the records of the State Motor Vehicle Department for duplicate matches and identification verification. There are three (3) full-time County elections staff. The Elections Director employs a Native American election outreach coordinator and an Elections Technician. Additional, temporary outreach employees are hired where necessary to assist with community outreach. They hire additional, part-time translators for Election Day. They have a monitor, an inspector, two judges, two clerks, a marshal and up to three (3) translators at each precinct. They do not have their own IT staff. They have an IT person from the County who assists them during elections to ensure that all systems are working properly.

5.1.1.4 Supported Elections

In Apache County, they have an intergovernmental agreement with the municipalities and districts to conduct elections and any election outreach activities. They have a joint technology district (NAVIT) and a hospital district that overlap with Navajo County.

The Navajo Nation conducts its own elections via the Navajo Election Administration. The County works with them for voter registration. The Nation uses a picture ballot which Arizona State statute does not allow.

5.1.1.5 Election Preparation

In Apache County, voter outreach is directed mostly toward Native Americans and includes registration drives. This is because Arizona is subject to Section V of the Voting Rights Act (VRA) that requires that the Department of Justice monitor many of its voting activities. Among them is the monitoring of its outreach programs to the Native American population to ensure that the opportunity for them to vote is not abridged by language barriers. Apache County, in fact, now has a higher percent of the population that is registered to vote than does the general population of Arizona.

In addition to the use of radio stations and newspapers announcements, Apache County also conducts demonstrations and presentations to the population. The County also conducts “Kids Voting” as an educational program. The County indicated that it will continue to place priority on Native American voter outreach and ballot translation. The County invites the DOJ to observe elections though it is no longer mandated by DOJ.

In Apache County, ballots are created by the Elections Director, who turns them over to Election Operation Services, Inc. for programming of the cards and management of printing and delivery.

In Apache County, the ballot is not created in Navajo (or any other native) language. If the ballot were written in Navajo, only about 10 percent of the Navajo population could read it. Navajo has traditionally been an oral language and is only now becoming a written language. County, tribal and community workers from Arizona, New Mexico and Utah, have developed a dictionary of voting related terms which is becoming the standard terms to be used in election-related education (to be added to the written language). County election staff conduct translation training and create audio tapes for use in assisting voters. Voters may request a translator from the County, or they may bring their own translator to vote. The average duration of a ballot translation for one voter is 45 minutes; however, it could be longer, depending on the ballot content. Because of an extensive translation requirement, absentee voting in Apache County is minimal. DREs that might be acquired to assist persons with visual impairment could also be used to assist Navajo people with a verbal translation of the ballot.

5.1.1.6 Early Voting

In Apache County, early voting is on the rise. Early voting envelopes are sent to the Recorder to verify registration, and then are sent to the Election Division. The Election Division keeps a log of early votes received during the outreach early voting drives, and they count the ballots before they are sent to the County Recorder. For those that may have voted early and then show up at the precinct to vote, there is a list that shows that they have requested an early ballot. They can vote provisionally, if they are shown on the early ballot list but insist that they have not voted.

5.1.1.7 Precinct Voting

In Apache County, they do logic and accuracy (L&A) testing for machines several days before the election. The Secretary of State does testing of central count machines and precinct machines. Voting equipment is tagged and sealed. Cards remain sealed until machines are returned. The machines are returned on election night. There is a receiving board for receiving the ballots and boxes. The Audit Board makes sure that the machine tape printout matches the ballots cast. The cards are not left in the machines if the transmission was not completed at the polling place. The entire election is backed up. In Apache County, batteries take 48 hours to recharge. They test the

batteries and replace them if required. They have an audit board that reviews the election by precinct. Provisional ballots are also counted and added to the final canvass. Paper ballots are stored for 24 months on federal elections. They have never had to use the stored ballots.

5.1.1.8 Precinct Voting Labor

In Apache County, they use county staff to distribute the voting equipment. Precinct inspectors are discouraged from taking the machines home and are encouraged to leave them securely locked at the polling place until Election Day. In Apache County, the Navajo outreach workers assist in poll worker training. They do mock elections for training and show them how to manage the precinct. They have as many as 2,300 active voters in the larger precincts.

5.1.1.9 Disabled Accessibility

In Apache County, DREs that might be acquired to assist persons with visual impairment could also be used to assist native Navajo people by providing a verbal translation of the ballot.

5.1.1.10 Central Count and Reporting

Apache County indicated that Diebold support has been good, but they were not happy that the certified version of GEMS (1.18.18) did not permit the printing of the Statement of Votes Cast (SOVC)¹. They were required to install the prior version of GEMS (1.18.15) in order to obtain this report. They use modems to transmit results to the central count area from designated collection centers. Voting machines are brought from precincts to the nearest collection center.

5.1.1.11 Vendor Management

In Apache County, they do not perform all of the equipment maintenance but instead send machines to Diebold if there are any maintenance issues. They have a maintenance agreement but no service levels established. They have an “800” number to call during elections for technical support.

¹ A standard and essential part of the GEMS application

5.1.2 Pima County

5.1.2.1 County Demographics

County	% of State Population (1990)	Population (2004) Estimate	Percent of State Population (2004)	Voter Registration March 2004	Voters as Percent of Population	Percent of State Registered Voters	Number of Precincts March 2004	Average Voters per Precinct
State	100%	5,130,632	100%	2,274,367	44%	100%	2,108	1,078
Pima	16%	843,746	16%	385,917	46%	17%	401	962

5.1.2.2 Elections Technology

County	Provider	Voting	Central Count	Ballot & Reporting
Pima	Diebold	AccuVote Optical Scan (OS) V-1.94	1) AccuVote Tabulator 2) Central Count Diebold Feeders V 2.0.12	1) AccuVote ES 2000 Firmware 1.94w 2) Global Election Management System (GEMS) V1.18.19

In Pima County, they have two (2) Dell servers that are not mirrored but they back up the first server onto the second server. They have created a backup solution involving an outside machine, but have never had to use it.

5.1.2.3 Elections Organization and Staffing

In Pima County, the County Elections Division is responsible for conducting all election administration, while the County Recorder is responsible for voter registration. The Elections Division reports to the County Administrator, who in turn reports to the Board of Supervisors. The Board makes the voting canvass official. The Board approves poll workers and polling places.

They hire 40 temporary staff (not poll workers) to work during major elections, for transport, warehouse operations, precinct trouble shooting, etc. They have an early voting board of ten (10) poll workers to observe and manage early voting. They have 2,300 poll workers (volunteer) to work at voting locations during major elections. They also have their own IT staff that maintain and repair their election equipment. They conduct electronic repair and also physical repair of equipment casings (casings cost as much as \$1,700 each to replace). They rely minimally on Diebold for maintenance.

5.1.2.4 Supported Elections

In Pima County, they have an intergovernmental agreement to conduct elections for Pima County municipalities, school districts and other election districts. The only exception to this is the City of

Tucson, which borrows County election equipment, runs its own election, and trains its own staff and volunteers. Political parties are allowed to submit in their own ballot tests for the Tucson municipal elections.

5.1.2.5 Election Preparation

In Pima County, they develop ballots (on GEMS) in-house and send them to a print file. The file is then sent directly to a printing firm for ballot production¹.

In Pima County, during Logic & Accuracy Testing, all machines are checked with full and blank ballots (350 machines). This occurs for both early voting and precinct voting. The County creates its own test ballots. They may have up to 1,700 different ballot types and must ensure that the correct ballot type is tested for each machine. They also test for ballot rotation. They create about 4,000 ballots in the test deck for use in testing the machines. In addition, they test their modems to ensure that they will work correctly. The SOS additionally tests machines. SOS tests approximately 10 percent of the voting machines and does not tell Pima County which machine they will test. In addition, SOS has a machine at their premises that they can also use for testing. Machines are sealed after testing.

In Pima County, language translation tapes are created and are made available to those that require them.

5.1.2.6 Early Voting

In Pima County, early voting is increasing as it is in most other counties.

5.1.2.7 Precinct Voting

In Pima County, once machines are tested, they are sealed and bagged. They log and print a receipt. The receipt validates that the data on a machine is correct. Voting machines are distributed to precinct inspectors at poll worker class. They sign for the machines and have the responsibility of transporting them to their own individual precincts. They have a ballot print order created and once ballots are printed, they are sent to the warehouse. Ballots and boxes are then sent to the precincts.

Election inspectors review the log of ballots that was created for them. They check that they have the appropriate number of ballot boxes. They have observers and have a good inventory system to avoid ballot irregularities from occurring.

5.1.2.8 Precinct Voting Labor

In Pima County, the County conducts all poll worker training. Poll workers are usually well trained to use the machines. They have a manual that the poll workers use. They do not have Diebold technical staff on site during elections, but Diebold staff are available via cell phone if needed. Pima County enters into a contract with the person who controls the precinct. The AccuVote tabulator is given to the inspector, who takes it home for safekeeping; it is sealed and opened on election morning. The rest of the equipment is locked, sealed and stored at the precinct. Tape printouts of counts are automatically generated when the AccuVote tabulator is activated. Neither

¹ The same firm is used by Maricopa County

the vendor nor any non-election workers have access to the AccuVote tabulator. Any software updates are physically mailed by the elections vendor to Pima elections staff for installation and testing.

5.1.2.9 Disabled Accessibility

In Pima County, they produce a sample ballot in large print, and they have ballot magnifiers at the polling places, but they do not use Braille¹. Voters who are unable to use these tools will be given assistance by two (2) poll workers².

Pima County is interested in new equipment that provides the artifact quality of optical scan ballots with the ease of use of DRE equipment as an ideal solution for future accommodation of voters with accessibility concerns. They recognize that they will need to obtain pre-clearance from DOJ to use such machines.

5.1.2.10 Central Count and Reporting

In Pima County, security starts at the main door of the central count location. They lock the doors but have laminate (bullet proof) glass to allow observation while preventing any security incidents.

Pima County was using GEMS version 1.17.21. SOS required all Arizona counties to move from their current version of GEMS to the State certified version (version 1.18.18). Like many other counties, Pima County then had to revert to version 1.18.15 in order to run the Statement of Votes Cast (SOVC) because version 1.18.18 had a bug in it that prevented this report from working. They have complained to the vendor and have been promised an upgrade for GEMS version 1.18.18 that will correct the SOVC bug by September 2004. In addition, they have printer layout issues with version 1.18.18. There is concern about the timeliness of version patches and the certification process duration.

Pima County has a very tight electronic transmission methodology. They have access controls on the dial-up lines, they monitor the modem activity on election night and they have automatic mechanisms to ensure that only one upload occurs from each polling place. Pima County posts results on the Internet by using external media (CD) to move results from election machine to Internet Web server (no electronic interface). They use FTP³ to send their results to the SOS. After the election, they make backups of memory cards, clear the cards and seal the machines. They do not store memory cards with election results still on them.

Pima County conducts a post-election L&A test. They test against the original count in the database to determine if the tabulation was correct. They do not perform an L&A test on the individual voting machines. They also conduct an audit in which they examine the SOVC and check for any trends to ensure that no anomalies have occurred. They store paper ballots for 24 months in accordance with State Statute. If an election is contested, it occurs only after election results are made official. The order to recount would be a judicial action and would designate the contest to be recounted. If a recount is necessary, it may take seven (7) days to locate the recount ballots.

¹ They have not gotten a request for Braille.

² Each from a different political party.

³ File Transport Protocol

Should a recount be necessary, Pima County has built a filter that will tabulate only the recount office.

5.1.2.11 Vendor Management

In Pima County, they seldom need the elections vendor technicians, as they maintain the equipment themselves. They do have a software contract with the vendor (but not one for election hardware¹). They do not have a service level agreement with the elections vendor. They maintain a very good relationship with the elections vendor technical staff and have known many of them for years. Vendor technicians are not usually on site. Pima County ensures that both the elections vendor and County elections IT staff are on call during elections in case of an emergency.

¹ They do have a maintenance agreement with Dell for Dell hardware.

5.1.3 Yavapai County

5.1.3.1 County Demographics

County	% of State Population (1990)	Population (2004) Estimate	Percent of State Population (2004)	Voter Registration March 2004	Voters as Percent of Population	Percent of State Registered Voters	Number of Precincts March 2004	Average Voters per Precinct
State	100%	5,130,632	100%	2,274,367	44%	100%	2,108	1,078
Yavapai	3%	167,517	3%	83,983	50%	4%	104	808

5.1.3.2 Elections Technology

County	Provider	Voting	Central Count	Ballot & Reporting
Yavapai	Diebold	1) AccuVote Optical Scan (OS) 2) AccuVote TS (10) DREs for early voting. Use Optical scan for absentee voting	Do not have central count	1) AccuVote ES 2000 Firmware 1.94w 2) Global Election Management System (GEMS) V1.18.18

5.1.3.3 Elections Organization and Staffing

In Yavapai County, the Election Director reports to the County Recorder and to the Board of Supervisors. The Recorder is responsible for both the elections and voter registration. They have three (3) full-time and one (1) part-time staff. They use six to eight poll workers per precinct.

They depend on their election vendor for IT support for the GEMS application and on County IT support for hardware and computer backup support. They do not have Diebold on site during elections, but they are available by telephone. County IT staff is on site during election night and on call when they are needed other times. They have County IT support in posting results.

5.1.3.4 Supported Elections

In Yavapai County, they do all the elections for all jurisdictions of the County. Yavapai County conducts elections every year on the consolidated election dates.

5.1.3.5 Election Preparation

Yavapai election staff is on the VRAZ-I committee which discusses voter registration issues and development of the current statewide system. They have a very “strong”¹ association of Counties and an even “stronger” association of Recorders.

¹ Active

In Yavapai County, election staff use the GEMS election program to create the ballot layout. These files are then sent to Election Operations Services, Inc. to review. Verified print files are then sent to the printer. The County then manages the printer for production and delivery.

Ballots are printed (as per State Statute) in English and Spanish. Yavapai County does not have native language translation.

5.1.3.6 Early Voting

Early voting is permitted (by statute) thirty-three (33) days before Election Day. Over 40 percent of voters vote early. Early voting mail-ins are tabulated using optical scan equipment. In addition, voters have a choice of using optical scan or DRE equipment for onsite early voting. In the last election, 1,500 voters used the DRE equipment. For DRE early voting, a voter must fill out and sign an affidavit; the information and signatures are verified by voter registration before a voter access card is issued to the voter.

Prior to the start of early voting, the County conducts a “Check System Setup” to confirm the equipment information, i.e., the machine serial number, time and date, diagnostic, test printer and test card reader. County staff conduct an overall L&A test, then the precinct L&A test is conducted on each unit with the appropriate ballots for the precinct. After this process is completed, the Secretary of State conducts its L&A test.

They cannot tally the early vote until SOS has conducted its L&A testing. The bulk of the early ballots are usually counted on the Saturday before Election Day; those received up to Election Day are also counted before the election. The early ballots received by 7 p.m. on Election Day and all provisional ballots are counted after Election Day when voter registration is finished verifying the early and provisional ballots. Yavapai county staff think that the L&A testing by the SOS is useful because it serves as a double-check on the County testing. As elections get larger, however, L&A testing might be more difficult to accomplish without additional time before Election Day.

5.1.3.7 Precinct Voting

In order to transport the election equipment and supplies, the County rents large trucks. The truck drivers are temporary staff, who have been trained by working at the warehouse with the equipment. Usually the County is able to get the same people from election to election.

The optical scan unit is in its own carrying case, sealed with a numbered seal. The outside of the packing box has been sealed with mailing tape and an official seal is placed across it. The ballots are secured in their packing boxes, placed in a supply box and locked with a small metal lock.

A log is kept of the numbered seals, indicating what the seals were used for and for which precinct. The seal numbers are also on the polling place supply list and ballot report for the poll workers to check. Most precincts have a secure location in which to store the equipment. Inspectors do not take the equipment home. In addition, the election equipment warehouse has a separate ballot room that is climate controlled. Keys to this room are held by two people, the Warehouse Supervisor and the Election Director.

Voters typically require only two to three minutes to vote using optical scan equipment. Machines are stored in an air-conditioned room, and they have a separate key for each election box.

5.1.3.8 Precinct Voting Labor

In Yavapai County, they have ten (10) troubleshooters assigned to resolve problems on Election Day. The troubleshooters work as much as possible in the warehouse in order to become familiar with the equipment and supplies; they also attend a poll worker training class and another training class the night before Election Day. The County provides a poll worker handbook for voting procedures on Election Day. In addition, there is a separate opening and closing card for the AccuVote that also provides trouble-shooting information.

5.1.3.9 Disabled Accessibility

Yavapai County uses DRE units for visually impaired voters. For the DRE voting unit, they have a headset and keypad that are plugged into the unit for use for the visually impaired. Right after the completion of the ballots, the County hires a translator who records the ballot information in both English and Spanish. The DRE is user-friendly for voters who may have a hard time holding a pencil in their hands. Yavapai County believes that its current solution meets HAVA requirements for voters with accessibility concerns. It typically requires about one (1) hour for a visually impaired person to vote without direct aid.

5.1.3.10 Central Count and Reporting

In Yavapai County, they do not have a central count solution. Results are transmitted via modem from the precincts to the standalone election central computer. On election night, the AccuVotes are returned to election central; the memory card is still sealed in the unit with a numbered seal. Machines with seals still on them are transported back to central count. (They do not back up the memory cards, because the memory cards are not supposed to be removed at this time. They do not remove the cards until after the canvass is completed.) They recently replaced the batteries and they log battery replacements to track the life of the battery.

They conduct post election L&A testing on extra equipment usually later in election week, but use the same GEMS software for that election to verify the count. The Test Deck is usually about 12 to 15 ballots per precinct; they test 10 to 12 precincts and therefore have less than 200 ballots per test deck. They test districts, candidate rotation, write-in vote spaces, over vote, blank ballots, etc. in accordance with statutes.

A recount was done on the optical scan ballots. They had to pick out the ballots by hand. Ballots are packed and sealed and kept for 24 months. They have never gone back to the ballots after the period (30 days) in which to contest the canvass has expired.

Recounts of elections have been conducted using the optical scan ballots. The appropriate ballots were retrieved by hand.

5.1.3.11 Vendor Management

In Yavapai County, vendor support has been good. The vendor support person has been the same person since 1998. The vendor support person is usually a “phone call away” on Election Day via a cell-phone number. Yavapai has a maintenance contract with the vendor but does not have a formal service-level agreement established.

5.1.4 Maricopa County

5.1.4.1 Demographics

County	Percent of State Population (1990)	Population (2004) Estimate	Percent of State Population	Voter Registration March 2004	Voters as Percent of Population	Percent of State Registered Voters	Number of Precincts March 2004	Average Voters per Precinct
State	100%	5,130,632	100%	2,274,367	44%	100%	2,108	1,078
Maricopa	62%	3,072,149	60%	1,329,076	43%	58%	1,058	1,256

During the 1990s, Maricopa County grew in population by 500,000 but declined by two percent of the State's population as other regions of the State increased more rapidly. Still, 58 percent of all registered voters in the State live in Maricopa County, making it by far the single largest County for voting and encompassing over half of the entire State's voters.

5.1.4.2 Elections Technology

County	Provider	Voting	Central Count	Ballot & Reporting
Maricopa	ES&S	Optech III-P (Eagle)	ES&S Optech Model IV-C	ES&S Unity V- 2.2 ETP Version 1.06AB

Maricopa decided to replace its punch card system with an optical scan system in 1994. They chose Business Recorders Corporation (BRC) — now Elections Systems and Software, Inc. of Nebraska (ES&S) — as their vendor, signed the contract in 1995 and conducted their first election with the ES&S system in 1996.

Maricopa Elections staff have expressed satisfaction with the ES&S equipment, although it is no longer the current technology of that vendor. Maricopa is able to maintain the equipment by buying pre-owned equipment supplied by the vendor. They believe that this approach will be sustainable for quite some time.

5.1.4.3 Elections Organization and Staffing

The Maricopa County Office of the Recorder manages elections. They have 53 permanent staff supporting elections and there are 26 IT staff that support both the election and the Office of the County Recorder. They use 7,700 poll workers for major elections. County election operations are funded separately from the rest of the County Recorder's Office.

5.1.4.4 Supported Elections

The Maricopa County Office of the Recorder/Elections is contracted by twenty-one (21) municipalities to conduct their elections. The County also conducts the election for school districts

and special taxing districts within the County. The Maricopa County Recorder supplies the City of Phoenix with the list of registered voters within the City. The City of Phoenix conducts its own elections using its own ES&S Optech Model IV-Cs. The City of Mesa mails its own Early Ballots, but the County processes and counts the ballots.

5.1.4.5 Election Preparation

Maricopa staff create the ballot layouts. Staff submit them to the print vendor (Runbeck Graphics) electronically via FTP. The FTP site is password protected. The County works directly with the print vendor to ensure timely delivery of both the early and regular ballots for the precincts. The ballot overruns are uncut sheets that are retained until after the election in the event of shortages. The printer is responsible for destroying overruns on ballots after authorization from the County. The unused early and precinct ballots are destroyed by the County. In accordance with State statute, ballots are printed in English and Spanish.

Prior to the election, an L&A test is performed on the elections equipment by the Elections staff. Subsequently, the SOS also conducts an L&A test. After successful completion of these tests and the approval of the representatives of the two major parties, the equipment is readied for the election.

5.1.4.6 Early Voting

The County uses the Videojet printing equipment to print and bar code early voting envelopes.

Approximately 50 percent of all ballots in Maricopa County are early voting/absentee ballots. In-person early voting is offered at 10–13 early voting sites through out the County. Approximately 27 percent to 30 percent of all eligible voters vote in the primary (about 370,000 votes). Thus, about 186,000 early ballots must be counted for the primary election and approximately 500,000 for the general election. All early voting is processed centrally at the Ballot Tabulation Center (BTC) using eight ES&S Optech Model IV-Cs. The County can count approximately 15,000 ballots per machine per business day. Early voting is gaining in popularity in Maricopa (and in the rest of the country), so that the time necessary to process early ballots can be expected to increase.

The central count tabulation equipment is connected to a Novell LAN, which is not connected to the County network, nor does it have any exposure to the Internet.

5.1.4.7 Precinct Voting

Portable ES&S Eagle voting machines are used by the County at each precinct. Each portable machine has a memory pack that stores vote totals. Each voting machine is configured with the appropriate ballot styles for a specific precinct before being sent to the precinct. Each machine is tagged and the memory pack serial number noted. The County is able to reconcile every machine in case of any errors in distribution. The memory packs are transported to one of 15 Memory Pack Sites (MPSs) after the polls have closed and the last voter in line has voted. The precinct vote totals are transmitted to the BTC using a Smart Pack Reader (SPR). There are approximately 140 precincts in each countywide election that modem the results directly to the BTC after the polls have closed and the last voter has voted.

5.1.4.8 Precinct Voting Labor

State statute stipulates that six (6) poll workers are to be allocated to each voting location. Maricopa County assigns eight (8) poll workers to those precincts requiring language assistance. This includes troubleshooters that are trained on the equipment (150 troubleshooters in total are deployed during an election). The vendor usually provides five (5) technicians on site to ensure proper equipment operation.

5.1.4.9 Disabled Accessibility

At present, Maricopa has limited facilities to accommodate voters with vision disabilities. Special Braille and large type ballots are developed by the County as requested, though there is a very small level of request for these special ballots. The County is considering using Automark technology with their current optical scan systems. This technology only reads and marks the ballot for disabled voters. The Automark does not tabulate ballots. The ballot will be fed into the Optech III-P at the precinct.

5.1.4.10 Central Count and Reporting

For the more remote precincts, voting machines are equipped with modems to send vote totals of the precinct to the Ballot Tabulation Center. There are over 100 machines that are so configured. Servers are used to collect all counts that are sent via modem (over 20 phone lines) to the BTC from the MPS centers and individual machines in the case of remote precincts. The BTC has an uninterruptible power supply (UPS), which will maintain electrical power in the event of utility company power outages (which rarely occur).

The County is routinely able to release election results shortly after 8:00 p.m. on Election Day. The physical ballots are retained for 24 months in accordance with State statute and in case it is necessary to conduct a recount.

5.1.5 Cochise County

5.1.5.1 County Demographics

County	% of State Population (1990)	Population (2004) Estimate	Percent of State Population (2004)	Voter Registration March 2004	Voters as Percent of Population	Percent of State Registered Voters	Number of Precincts March 2004	Average Voters per Precinct
State	100%	5,130,632	100%	2,274,367	44%	100%	2,108	1,078
Cochise	2%	117,755	2%	51,414	44%	2%	64	803

5.1.5.2 Elections Technology

County	Provider	Voting	Central Count	Ballot & Reporting
Cochise	ES&S	ES&S Model 100	ES&S Model 150 (Central Count) 150 ballots/min.	ES&S Unity Version 1.0 (ERS 6.3.10)

Unity election equipment is not connected to the Internet or County LAN.

5.1.5.3 Elections Organization and Staffing

In Cochise County, the Elections/Special Districts Office under the County Administrator (who reports to the Board of Supervisors) is responsible for the conduct of elections while the County Recorder is responsible for voter registration. The Elections/Special Districts Office has two (2) full-time staff. The Elections District does not have its own IT staff. They have one County IT staff member who assists them with maintaining and operating the servers and who runs the computers on Election Day.

5.1.5.4 Supported Elections

The County conducts elections for all municipalities and districts within the County.

5.1.5.5 Election Preparation

In Cochise County, because of the small staff, they rely on elections consultants (Election Operations Services, Inc.) to create ballot layouts, order and manage ballot printing, and program the memory cards for each election. They considered having this work done by ES&S, but found that it was prohibitively expensive. Ballots are printed in both English and Spanish in accordance with State statute. There are no Native American reservations in Cochise County and therefore they do not provide oral translation of ballots.

In Cochise County, all individual machines are tested with both the precinct memory cards to be used on Election Day as well as the backup memory cards to be used in case the primary memory card should fail. Test ballots are used on all the machines. For the SOS L&A test, enough machines are chosen for the test to ensure that all ballots with the different candidates are tested.

In addition, the tape of a machine's SOS L&A test is compared with the results of the County's L&A test to ensure that results are the same.

5.1.5.6 Early Voting

Early votes are received by the Recorder's Office; signatures are then verified there. Once verified, the early ballots are sent to the Elections Director's office for processing and tabulation after the L&A test is completed a few days before Election Day.

5.1.5.7 Precinct Voting

Sealed and bagged equipment is sent to the precincts. Precinct inspectors may take the voting equipment home overnight if the precinct involved is not a secure site.

5.1.5.8 Precinct Voting Labor

In Cochise County, they have six (6) poll workers at each precinct in accordance with State statute. They have metal ballot boxes, which are very heavy and bulking and thus difficult to transport.

5.1.5.9 Disabled Accessibility

The County has magnifiers in the polling places to assist those with certain types of vision problems. They also have clip-on lights in the disabled voter booths. They are trained to do "curbside voting." No one has yet requested an audio version of the ballot. They would like a DRE that marks a paper ballot as their solution for accessibility requirements of HAVA for 2006. They would like to avoid any interoperability issues when they purchase a DRE for disabled voting.

5.1.5.10 Central Count and Reporting

In Cochise County, votes are counted at the precinct, and the results are then transmitted over modem to the central count area.

5.1.5.11 Vendor Management

The County has a maintenance and warranty contract with ES&S, but they do not have explicit service levels stipulated in the contract.

5.1.5.12 Improvements

The County would like to see SOS training focused on issues faced by the smaller counties. They would like a state-managed voter registration system to make the registration management process more efficient. They feel somewhat at risk with only a few resources trained in programming memory cards and ballot layouts.

5.1.6 Graham County

5.1.6.1 Demographics

County	Percent of State Population (1990)	Population (2004) Estimate	Percent of State Population	Voter Registration March 2004	Voters as Percent of Population	Percent of State Registered Voters	Number of Precincts March 2004	Average Voters per Precinct
State	100%	5,130,632	100%	2,274,367	44%	100%	2,108	1,078
Graham	1%	33,489	1%	14,678	44%	1%	18	815

5.1.6.2 Elections Technology

County	Provider	Voting	Central Count	Ballot & Reporting
Graham	ES&S	ES&S Model 100		ES&S Unity Version 1.0 (ERS 6.3.20)

Graham County does not need special central count equipment due to the limited size of its voting population. They use the Model 100 as both a precinct-based, voter-activated paper ballot counter and vote tabulator. Their equipment is one year older than the system deployed in Cochise County.

5.1.6.3 Elections Organization and Staffing

In Graham County, the Office of the County Manager has an Elections Coordinator that is responsible for all County elections. This position is also responsible for all accounts payable, inventory, worker compensation claims and various other full-time duties, and is therefore not a full-time position dedicated to elections. The County Recorder is responsible for voter registration and for managing and counting early voting. Other County Manager staff assist during elections. They hire 108 poll workers for precinct voting and have six (6) central counting board workers for both early ballot counting and election night counting. Graham County has one IT staff resource from the County IT Department (there is a total of three County IT staff) who manages computer and software setup for elections.

5.1.6.4 Supported Elections

In Graham County, they have an agreement with Safford City to conduct elections on its behalf. They also conduct elections for county schools and other districts.

5.1.6.5 Election Preparation

In Graham County, because of the small elections staff, they also rely on elections consultants (Election Operations Services, Inc.) to create ballot layouts, order and manage ballot printing and program the memory cards for each election. They do not have a purchase order issued for services to Election Operations Services, Inc. EOS simply invoices the County for the services rendered.

In Graham County, they conduct L&A testing for all machines. They test using marked ballots and use an average of 50 test ballots. The SOS conducts the testing on the Thursday or Friday before the election.

5.1.6.6 Early Voting

In Graham County, early voting is supervised/conducted by an early voting board of election workers. The Elections Coordinator prepares the machines for early voting. The County Recorder conducts early voting, because the recorder verifies the mailed-in ballots against the voter registration file.

5.1.6.7 Precinct Voting

In Graham County, they have 22 Model 100 voting machines (four extra machines). They have a special requirement in that the Gila School District crosses County boundaries, so they provide the District with Graham totals and final results are tabulated outside of Graham County.

5.1.6.8 Precinct Voting Labor

In Graham County, County custodial staff and highway staff deliver the election equipment to the precincts. The County Sheriff's deputies bring in the ballots on election night. Equipment is always locked and sealed before delivery. The inspector is in charge of equipment, but does not take it home. All the equipment is locked at that precinct. Six (6) board poll workers are assigned to each precinct as per State statute. Voters feed their own ballots into the counters.

5.1.6.9 Disabled Accessibility

In Graham County, they supply magnifiers to the polling places. Some people found the ovals were printed too lightly; now they are printed darker. To the knowledge of current staff, Graham County has never had a blind voter. They have home voting for the disabled, if required. Two representatives will visit and provide assistance. Graham County poll workers will help a person vote curbside if requested to do so; this assistance is provided by one poll worker of each party.

5.1.6.10 Central Count and Reporting

In Graham County, all ballots and cards are brought physically to the central count. They are in the process for establishing electronic transmission of election results, hopefully for September 2004 deployment. Election results are read off the card and they are tabulated on the central count computer. The results are sent by FTP to the SOS.

In Graham County, memory cards are stored with all their information intact until the next election. They do not monitor battery life. There is no indication when batteries will fail. Ballots are stored in the Treasurer's vault for two years (in keeping with State statute) and they also store unused ballots. Graham County has recently purchased all new PCMCIA cards with replaceable batteries. All election information is also printed on a hard copy; the floppy disk with the election definition is also saved.

5.1.6.11 Vendor Management

In Graham County, they have a good relationship and receive satisfactory service from ES&S. They have an annual maintenance agreement where voting equipment is serviced every year prior

to the election cycle. ES&S will take a scanner back to their facility if it cannot be repaired on site, and will ship it back if necessary. The vendor sends a survey to determine if maintenance is required. One time they had a machine “go down,” and ES&S simply replaced it with another machine. They do not have established service levels with ES&S. They had an ES&S person on site for the first year the system was deployed, but now they have an “800” number that they may use during elections.

5.1.6.12 Improvements

In Graham County, provisional ballots are verified and counted on election night while the night poll boards are present. If there are additional provisional ballots to be counted the following day, they are counted in the presence of a republican and democrat from other departments. Thus far, the equipment and processes they have used have worked without any problems, and they are very satisfied with both.

In Graham County, they feel the State Elections Manual could be more prescriptive and less open to interpretation. They would like the SOS to provide information or advice to the counties for such things as campaign finance. County attorneys may not have the legal expertise for issues like campaign finance.

Graham County would like early voters that come into the Recorder's Office to vote to be able to run their ballot through the scanner and have it counted on the spot. This would eliminate hundreds of early ballots that need to be opened, sorted and counted by the early boards. It will also eliminate duplication, because the scanner gives the voter the opportunity to make any corrections while they are present. Therefore, the County would like the SOS L&A testing to be performed earlier. At the very least, the program could be tested earlier by the SOS and the County could then continue to test the equipment in preparation for early voting.

5.2 Analysis and Recommendations

In review of the interviews conducted with the selected Arizona counties, it is clear that there are certain recurring issues among the selected counties. Below, these issues have been summarized and recommendations have been added to each of them.

5.2.1 SOS Public Outreach

5.2.1.1 Analysis

Arizona counties do not rely solely upon election vendor personnel, or solely upon the safeguards built into the election equipment, but also use a series of “check and balance” procedures to ensure that elections are accurate.

5.2.1.2 Recommendations

- 1) SOS should perform outreach to voters who question the veracity of election methods. This will minimize concern and trust issues in the public and media. The public should understand how these election procedures protect the results of elections.
- 2) SOS should issue a direct statement addressing this issue. SOS should ensure the public is informed about election systems and procedures.

5.2.2 SOS County Training, Certification and Qualifications

5.2.2.1 Analysis

SOS training requirements differ between large, medium and small counties. Large counties are interested in campaign finance law and other more arcane items, while small counties are interested in better training on the process of elections. Collaboration between SOS and counties is very important. The recent implementation of statewide voter registration was an example of good collaboration between them. County staff, especially from large counties, can contribute to the training of all county staffs.

In addition, the state elections procedures manual was a great idea. Counties would like to see it continued, expanded and kept current.

Background checks of election staff and poll workers may be worth considering to ensure that an incident that might undermine public confidence in voting does not occur.

5.2.2.2 Recommendations:

- 1) SOS should continue the outreach approach it used in voter registration, as it was very effective in gaining county cooperation.
- 2) SOS should enhance its training programs so that they are targeted at the issues of concern to various-sized counties.
- 3) SOS should consider background checks for elections staff and poll workers in keeping with heightened awareness of election security.

5.2.3 Variations of Election Organizations in Counties

5.2.3.1 Analysis

The Counties vary as to how they are organized to conduct voter registration and voting. Some counties have a County Recorder who is elected and an Elections Director who is appointed by the Board of Supervisors. In other Counties, such as Maricopa, Navajo, Coconino and Yavapai, both roles are under the County Recorder. The two functions are separate; one is to ensure that only eligible voters are able to vote. The other function counts the votes. With early voting, provisional balloting and precinct registration validation, there are intertwined business processes between the two functions.

5.2.3.2 Recommendations

- 1) Arizona should consider a uniform organizational approach to election management for all counties.
- 2) Arizona should ensure that elected officials are not placed in a position where the perception of inappropriate motives could cloud the professionalism of the election process.

5.2.4 Arizona/Wyoming Ballot Rotation

5.2.4.1 Analysis

There is a unique election requirement (done only by Arizona and Wyoming) in which ballot rotation is required to occur in a certain manner not common among other states. Election vendors must provide for this unique requirement when upgrading their election software. This adds an additional item to the certification process that would not be reviewed by the ITAs.

5.2.4.2 Recommendations

SOS should certify election equipment specifically for Arizona/Wyoming Ballot Rotation.

5.2.5 Ballot Creation Single Points of Failure

5.2.5.1 Analysis

Ballot creation and memory card programming is done by a two-person firm, Elections Operations Services, Inc. for most Arizona counties. Some counties rely on them very much, while other counties use them only to broker printing. The nine (9) counties that recently received new Diebold election equipment have been trained on the equipment so that the statewide reliance upon this small firm has been reduced.

5.2.5.2 Recommendations

- 1) The State should consider ways in which it can mitigate risk of a single, small vendor providing county services for ballot design, memory card programming and printing coordination throughout the State. One mitigation approach would be to ensure that there are several government staff throughout the counties that perform these functions and could do so for neighboring smaller counties, if necessary.
- 2) SOS should work with counties to ensure a contingency plan should Elections Operations Services be unable to perform its functions.
- 3) SOS should encourage counties to develop ballot creation skills.

5.2.6 Languages

5.2.6.1 Analysis

Apache County has a very large Navajo population, many of whom are not literate in English. Thus, Apache County has a great need for oral translations into Navajo. In accordance with State law, the ballot material in Apache County is in both English and Spanish, though there is little need for Spanish in the County.

5.2.6.2 Recommendations

- 1) SOS should continue to support counties with Native American populations with oral translation efforts.
- 2) As Spanish and English are mandated, SOS should make no changes in those requirements.

5.2.7 “Bug” in Certified Version

5.2.7.1 Analysis

The current certified version of GEMS 18.18 has a “bug” (i.e. “error”) that required fallback to a prior version (18.15) in order to run the Statement of Votes Cast (SOVC) Report — all GEMS counties complained about this.

5.2.7.2 Recommendation

SOS should review version 18.19 for completeness and accuracy and then certify it for all Arizona GEMS counties.

5.2.8 Early Voting

5.2.8.1 Analysis

There is a trend among voters in Arizona (and across the nation) toward ever-increasing participation in early voting. Yavapai County experiences 60–65 percent turnout through early voting. Counties are generally in favor of early voting, as it decreases the pressure on them on Election Day. For a variety of reasons, it is more difficult to get qualified and available poll workers. Early voting could also ease this labor issue.

5.2.8.2 Recommendation

SOS should promote early voting by mail and have more outreach to encourage early voting.

5.2.9 Election Processing Single Point of Failure

5.2.9.1 Analysis

Very few IT professionals are involved in the process in each county. There is heavy reliance on one person in several counties.

5.2.9.2 Recommendation

SOS should work with counties to ensure inter-county technical support, and ensure intra-county backup technical support.

5.2.10 Flaw in L&A Testing Method

5.2.10.1 Analysis

With DRE it is possible for fraud to be programmed for a certain date, time and count that would not be detected with current L&A. What is needed is a certification process for vendor programmers and tracking of software from vendor to election. There is an L&A Mode and an Election Mode in which equipment can be tested. Concern is that a defect or fraud could exist in Election Mode, but not in L&A Mode.

5.2.10.2 Recommendations

- 1) L&A testing should be done in election mode if at all feasible for both optical scan and DRE equipment.

2) On the date and time issue, see the section of this report on software security.

5.2.11 Voter Verifiable Paper Audit Trail (VVPAT)

5.2.11.1 Analysis

Yavapai County is currently the only Arizona county using DRE voting equipment, but they find the equipment has numerous advantages. Prescott, for example, has voters of all age groups, and older people actually like the DRE as it is simple to operate and can be easily read. They appreciate the ease with which they can correct their ballot. There is some concern with adding VVPAT as voters may wish to change their ballots once they see their printouts. This could cause election count and accuracy issues.

5.2.11.2 Recommendation

See recommendations regarding VVPAT in Section Two (2) of this report.

5.2.12 Short Ballot Window

5.2.12.1 Analysis

Pima County does not have enough time between SOS L&A test and Election Day to process absentee ballots. For Maricopa County, very large elections can result in 7,000 ballot styles. Their central tabulators may be over burdened by this. This is resolved by splitting the election counting among the tabulating machines. At present, State L&A testing occurs seven days before the election. Especially for Pima (and Maricopa) County, this means that all early voting (an increasing proportion of ballots) must be completed within those days prior to Election Day. From the State's perspective, there should not be too much time elapsed between state L&A testing and the conduct of the election.

5.2.12.2 Recommendations

- 1) SOS should continue to have a seven-day window to ensure equipment is checked as close as possible to Election Day.
- 2) SOS should assist large counties with acquisition of sufficient central count equipment to ensure that all elections are processed within the window.

5.2.13 Battery on Card

5.2.13.1 Analysis

Memory card batteries go bad. Counties differ on their understanding of their memory life and on approach to management of this.

5.2.13.2 Recommendations

- 1) SOS should work with the counties to determine a statewide standard for battery management including inventory and replacement.
- 2) SOS should ensure that counties that replace batteries (or other components) with exactly the item that was certified so as to comply with certification process.

5.2.14 Retention of Memory Card Data

5.2.14.1 Analysis

Some counties leave cards in the machine until the next election, while other counties remove the card and copy its image onto servers and then erase the card's memory. Pima County, for example, is not clear on the state policy regarding memory card management. Are they to store the memory cards and information for 24 months? Currently they make backups on a computer and erase the memory cards.

5.2.14.2 Recommendation

SOS should work with the counties to determine a statewide standard for memory card management including backup and storage.

5.2.15 Solution for Disability

5.2.15.1 Analysis

Non-DRE counties with ES&S equipment are considering Vogue Voting System's AutoMark device as a non-DRE solution to accessibility. Yavapai County is happy with its current early voting DRE solution.

5.2.15.2 Recommendation

The solution to accessibility is a requirement in 2006. SOS should examine all viable alternatives and prepare to make a selection that meets HAVA accessibility requirements.

5.2.16 Post Election L&A Testing

5.2.16.1 Analysis

None of the counties perform L&A after the election (except on some central count machines). A post-election L&A is not required by law, but is indicated in the State elections manual as advisable.

5.2.16.2 Recommendation

SOS should ensure that counties conduct a post election L&A. Counties should conduct exactly the same test using the same test decks as before the election. This will establish that no changes in the behavior and performance of the equipment have occurred since the pre-election L&A.

5.2.17 Two-Year Retention Requirement

5.2.17.1 Analysis

All counties questioned the State requirement to retain ballots for 24 months after the election, noting that election results are official within perhaps 30 days of election.

5.2.17.2 Recommendation

SOS should consider legislation to revise this requirement to a shorter time frame. There appears to be no purpose in a 24-month requirement as the time for contesting of an election expires within a month or two of the election.

5.2.18 Legal Advice Source

5.2.18.1 Analysis

Counties are redirected by SOS to County Counsel for legal advice. Often County Counsel is not familiar with issue and refers it to other County Counsel, SOS or to Attorney General. There needs to be a central focus point for this that draws on all of State and county legal resources and provides uniform answers for all counties.

5.2.18.2 Recommendations

- 1) SOS should encourage CERA certification for all county attorneys. This would enable them to make knowledgeable assessments of election issues.
- 2) SOS should facilitate periodic workshops with Attorney General, county attorneys and SOS staff regarding election legal issues.

5.2.19 SLAs Are Lacking in Vendor Contracts

5.2.19.1 Analysis

None of the counties have service-level agreements with their elections vendors. They rely on service contracts without explicit service levels or personal relationships to ensure that they receive services when needed.

5.2.19.2 Recommendation

SOS should encourage counties to include SLAs in all future election system contracts and should assist them in developing SLA standards.

5.2.20 Continuity Planning and Disaster Recovery

5.2.20.1 Analysis

The degree of awareness and preparation to ensure election processing in an emergency varies widely among the counties. In most counties, the equipment is not anchored and may not be supported by uninterruptible power supplies (UPS). There is usually no contingency plan or alternate equipment for vote counting should central count be unavailable.

5.2.20.2 Recommendations

- 1) There are a number of fundamental disaster preparedness tasks that should be undertaken by all counties.
- 2) SOS should set minimum standards of preparedness for all counties in collaboration with them.



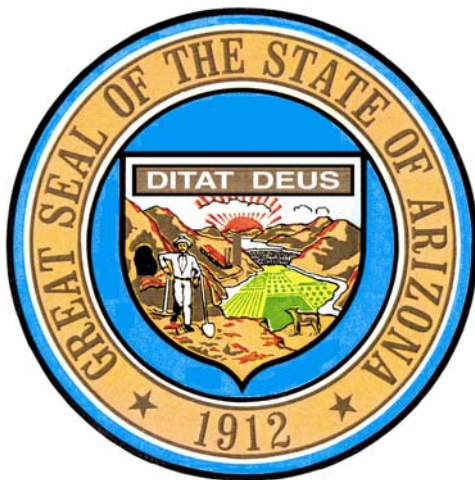
A Report for the

State of Arizona

Assessment of Election Systems – Appendices A-E

December 2004

Engagement: 220608071



research consulting measurement community news

Gartner

Table of Contents

- Appendix A: Summary of County Statistics 2**
- Appendix B: Best Practice Certification Procedures 3**
 - 1.1 Process for Application 3
 - 1.2 Process for Evaluation 3
 - 1.3 Process for Approval or Rejection 4
 - 1.4 Certification of System Configuration 5
 - 1.5 Changes to Certified System Configuration 5
 - 1.6 Process for De-certification 6
- Appendix C: Recommended Minimum Voting Machine Requirements 7**
 - 1.1 Operation 7
 - 1.2 Security 7
 - 1.3 Storage and Transportation 8
 - 1.4 Electrical 9
- Appendix D: State of California Certification Procedures 10**
- Appendix E: State of Louisiana Certification Procedures 38**

Appendix A: Summary of County Statistics

County	Provider	Population (1990)	Percent of State Population	Population (2004) Estimate	Percent of State Population	Voter Registration March 2004	Voters as Percent of Population	Percent of State Registered Voters	Number of Precincts March 2004	Average Voters per Precinct
Apache	Diebold	61,591	1%	69,423	1.35%	39,083	56%	2%	45	869
Cochise	ES&S	97,624	2%	117,755	2.30%	51,414	44%	2%	64	803
Coconino	Diebold	96,591	2%	116,320	2.27%	63,555	55%	3%	83	766
Gila	Diebold	40,216	1%	51,335	1.00%	24,932	49%	1%	40	623
Graham	ES&S	26,554	1%	33,489	0.65%	14,678	44%	1%	18	815
Greenlee	Diebold	8,008	0%	8,547	0.17%	4,088	48%	0%	8	511
La Paz	Diebold	13,844	0%	19,715	0.38%	6,720	34%	0%	12	560
Maricopa	ES&S	2,551,765	62%	3,072,149	59.88%	1,329,076	43%	58%	1058	1,256
Mohave	Diebold	93,497	2%	155,032	3.02%	83,874	54%	4%	73	1,149
Navajo	Diebold	77,658	2%	97,470	1.90%	50,587	52%	2%	70	723
Pima	Diebold	666,880	16%	843,746	16.45%	385,917	46%	17%	401	962
Pinal	Diebold	116,379	3%	179,727	3.50%	73,256	41%	3%	67	1,093
Santa Cruz	Diebold	29,676	1%	38,381	0.75%	17,973	47%	1%	24	749
Yavapai	Diebold	107,714	3%	167,517	3.27%	83,983	50%	4%	103	815
Yuma	Diebold	121,097	3%	160,026	3.12%	43,231	27%	2%	42	1,029
Total		4,109,094	100%	5,130,632	100%	2,272,367	44%	100%	2,108	1,078

Appendix B: Best Practice Certification Procedures

1.1 Process for Application

1.1.1 Eligibility

- 1.1.1.1 Any person or corporation otherwise qualified to do business in the State of Arizona and with self-certification to be capable of producing voting systems that meets the requirements of the state may apply for state certification.
- 1.1.1.2 Applications may be filed at any time in the form prescribed by the SOS.

1.1.2 Filing of Application

- 1.1.2.1 Applications must be completed in full and all filing fees paid before the evaluation process can begin unless waived by SOS.

1.1.2 Submission of Materials

- 1.1.2.1 Submissions may be filed in person at the Secretary of State's office in Phoenix, via common carrier (such as the United States Postal Service), or electronically via email. Forms for electronic submissions must be in Adobe Acrobat (.pdf) format.
- 1.1.2.2 At the discretion of the SOS, the applicant shall demonstrate the voting system identical to that which would be sold in the state if the application is approved. There must be sufficient quantities of expendables for SOS to adequately test the voting system.
- 1.1.2.3 Test ballots must be identical in format to ballots that would be used in actual elections conducted in the State.

1.2 Process for Evaluation

1.2.1 Considered Elements

- 1.2.1.1 The voting system must successfully complete the scripted demonstration and meet all the requirements outlined in the Voting System Requirements Appendix

1.2.2 Demonstration

- 1.2.2.1 Systems demonstrated must use exactly the same hardware, firmware and software as the systems that will be used State and local elections.
- 1.2.2.2 Demonstrations shall be held at the location and time decided by the Secretary of State. More than one vendor may be asked to demonstrate its system on any given date.

- 1.2.2.3 Applicants may be given a demonstration script. Applicants must complete the entire script.
- 1.2.2.4 Applicants may also demonstrate additional features of the product after completing the script.

1.3 Process for Approval or Rejection

1.3.1 Examination and Testing Process

- 1.3.1.1 The application will be examined for completeness. Incomplete applications will not be processed.
- 1.3.1.2 Prior applications from the same vendor may be reviewed.
- 1.3.1.3 The applicant must provide the EAC System Number and all applicable ITA Reports as proof that the same system has been certified under the Election Assistance Commission and NASED process.
- 1.3.1.4 The voting system must meet all of the items in the "Voting System Requirements" list

1.3.2 Provisional Approval

- 1.3.2.1 Provisional approval is conditional certification subject to rectification of deficiencies noted by SOS.
- 1.3.2.2 Provisional approval may be granted to those systems that meet the requirements with changes as noted by the Secretary of State.
- 1.3.2.3 Systems with provisional approval may be demonstrated and sold within the state, but must not be used until the provisional requirements have been satisfied.

1.3.3 Withdrawal of Application

- 1.3.3.1 The applicant may withdraw an application at any time before the process is completed.
- 1.3.3.2 The request for withdrawal must be in writing to the Secretary of State and will become effective when accepted by the Secretary of State.
- 1.3.3.3 Applicants shall forfeit all fees paid in case of withdrawal.

1.3.4 Notification of Decision

- 1.3.4.1 The applicant will be notified of the Secretary of State's certification approval/denial or provisional approval decision in writing.

1.3.5 Appeal Process

- 1.3.5.1 If an application is denied, the applicant may file an appeal within 30 days.

- 1.3.5.2 Appeals will focus on material disagreements of either completeness of the application or performance against the Voting System Requirements.

1.3.6 Escrow

- 1.3.6.1 Only those systems that have successfully or provisionally completed the evaluation process may be used within the State for state and local elections.
- 1.3.6.2 Units that are provisionally approved must complete the provisions within the appropriate timeframe or the approval will expire.
- 1.3.6.3 Before a voting system may be used in a State election, the vendor must place all application source code into either public domain or software escrow, and authorize the state as recipient of escrow.

1.3.7 Reapplication

- 1.3.7.1 Applicants that have withdrawn applications can reapply at anytime.

1.4 Certification of System Configuration

- 1.4.1 The entire configuration of hardware, software and firmware shall be certified as a unified voting system.

1.5 Changes to Certified System Configuration

1.5.1 Changes to Operating System or Third Party Software

- 1.5.1.1 Commercial Operating System - Security patches and operating patches to commercially available computer operating systems by shall be self-certified by the applicant, and do not have to be re-certified by SOS.
- 1.5.1.2 Commercial Third Party Software - Security patches and operating patches to third party commercially available software, shall be self-certified by the applicant, and do not have to be re-certified by SOS.
- 1.5.1.3 Custom Operating System or Custom Third Party Software- Custom operating system or custom third party software and the associated operating and security patches must be certified. The patches may only be distributed after the patched system has been re-certified.

1.5.2 Changes to Hardware

- 1.5.2.1 Modifications to product lines of commercially available computing platforms that do not materially effect the operation of the system shall be self-certified by the vendor.
- 1.5.2.2 Modification to product lines of custom designed computing platforms must be re-certified.

1.5.2.3 Modifications to firmware shall be treated as a modification to software.

1.5.2.4 Modifications to hardware used for vote casting or counting must be re-certified.

1.5.3 Changes to Voting System Application Software

1.5.3.1 Any upgrades or patches to voting system application software must be certified.

1.5.4 Emergency Conditional Certification

1.5.4.1 Definition of Emergency Conditional Certification (ECC) – Conditional Certification of voting systems that have been used and subsequently upgraded and that the SOS has determined are necessary for the successful conduct of a State or local election.

1.5.4.2 Should the state or a local jurisdiction require emergency patches to their voting system, the vendor may apply to the SOS for an Emergency Conditional Certification.

1.5.4.3 The ECC application shall include a description of the changes made since certification and the reasons why such changes warrant an emergency certification. The vendor shall also notify all affected jurisdictions within the State of its application for ECC.

1.5.4.4 An ECC shall be valid for a specified period of time as determined by SOS, after which it automatically expires.

1.6 Process for De-certification

1.6.1 Material Breach

1.6.1.1 The vendor's voting system may be subject to de-certification as a result of any material breach in its contract with the state or any of its jurisdictions.

1.6.1.2 Voting systems that are de-certified may be (but not necessarily will be) reinstated when the material breach has been addressed to the satisfaction of the Secretary of State.

1.6.2 Ineligible Application

1.6.2.1 Any material misrepresentation later discovered on an initial application may result in the de-certification of the voting system for use within the State.

1.6.3 Failure to Perform

1.6.3.1 If the voting system fails to perform or fails to meet guidelines for accuracy, dependability or security, the system may be decertified by SOS.

Appendix C: Recommended Minimum Voting Machine Requirements

1.1 Operation

1.1.1 Provide for Vote Recording

- Allow vote recording for or against/yes or no for initiative questions
- Provide for Arizona/Wyoming ballot rotation.
- Allow the voter to pick up to the appropriate number of candidates in each race.
- Clearly identify under-vote situations to the voter, but permit the voter under-vote
- Prevent over-voting
- Store votes cast even in case of power loss or other equipment failure, short of destruction of the machine, paper trail, and memory devices

1.1.2 Provide Vote Reporting

1.1.3 Create printed and electronic results at the end closing of the polls, on demand by authorized officials

1.1.4 Create summary report of votes cast for each device

1.2 Security

1.2.1 Provide printed records poll opening and closing reports as follows:

1.2.2 Identification of election

1.2.3 Identification of each unit

1.2.4 Identification of ballot format

1.2.5 Identification of candidates and/or issue, verifying zero start

1.2.6 Identification of all ballot fields and all special voting options

1.2.7 The system should provide an audit report on all attempts to access reporting or administration functions

1.2.8 The system should prevent unauthorized access

1.2.9 The system should prevent operations in an improper sequence

consulting

Gartner

- 1.2.10 The system should be not allow unauthorized media to be introduced, particularly during elections.
- 1.2.11 Assembly and access points on the system should be secured with locks and/or tamper-proof tape.
- 1.2.12 Provide for secret ballots
- 1.2.13 Prevent the voter from voting more than the appropriate time on the same candidate race or on the same question.
- 1.2.14 Permit all unused vote indicators or devices to be locked per question or ballot, as appropriate.
- 1.2.15 Provide a public counter or tabulator that at all times during the election shall show the number of persons who have voted.
- 1.2.16 Contain one or more automatic locks that upon exposure of the vote count at any time after the polls are opened on Election Day will automatically lock the machine against further operation unless authorized.
- 1.2.17 Provide a screen, hood, or curtain to provide for a secret ballot.
- 1.2.18 Be incapable of being reset, altered, or used except by authorized personal in the correct sequence.
- 1.2.19 Provide for protective counter that advances each time the system reset is performed.

1.3 Storage and Transportation

- 1.3.1 Have maximum weight to be handled by the poll worker while moving the voting machine or setting up the voting machine of not more than twenty-five (25) pounds
- 1.3.2 Be able to withstand a maximum temperature of 130 degrees Fahrenheit, while in storage, and 105 degrees Fahrenheit while in operation, and a minimum temperature of –15 degrees Fahrenheit, while in storage, and 40 degrees Fahrenheit, while in operation, without any permanent damage, degraded reliability or performance deterioration
- 1.3.3 Be able to survive exposure to uncontrolled temperature and non-condensing humidity environments, while in storage, and shall operate without damage to the component parts when operated at non-condensing relative humidity of up to 98%
- 1.3.4 When packaged for transportation, be able to reliably function after a 3 foot fall to a concrete surface.

1.3.5 When packaged for transportation, be able to reliably function after brief exposure to rain, snow, or other inclement weather conditions.

1.4 Electrical

1.4.1 Have a main power system and battery charger that operate from a standard 115-volt, 60hz, single phase, alternating electrical current.

1.4.2 Have a self-contained, internal battery backup that is rechargeable by the main power supply when the voting machine is plugged into AC power. This battery must be commercially available. The battery supply must be capable of operating the voting machine without AC power for at least 4 hours while powering all necessary components

1.4.3 Have a visible indicator that shows if the voting machine is receiving AC power. The voting machine must be able to test the battery and show the battery charge level. The voting machine must automatically shut itself down in the event the backup battery has only enough power to print out the results and go to an inactive state so to conserve enough power to close the polls at the end of the day and must provide an visual and audible alert should it switch to battery power.

1.4.4 Remain operable with no data loss in the event of abnormal line voltage conditions of power surges up to 132.25 volts rms over periods of up to two (2) seconds with a maximum of two (2) such surges per 60 second period

Appendix D: State of California Certification Procedures

Procedures for Approving, Certifying, Reviewing, Modifying, and Decertifying Voting Systems, Vote Tabulating Systems, Election Observer Panel Plans, and Auxiliary Equipment, Materials, and Procedures.

Table of Contents

Article 1. Introduction

Article 2. Jurisdiction

Article 3. Voting Systems and Procedures Panel, Advisory Committee, and
Technical Consultants

Article 4. Application for Approval and Certification

Article 5. Evaluating Applications

Article 6. Criteria for Approval or Certification

Article 7. Examination and Testing

Article 8. Modifications and Re-Examination

Article 9. Public Hearing

Article 10. Decision of the Secretary of State

Article 11. Periodic Review of Voting Systems

Article 12. Decertification of Voting Systems and Vote Tabulating Systems

Article 13. Acceptance Testing

Article 14. Maintenance Logs

Article 15. Biennial Tests of Voting Equipment

Article 16. Adoption of Federal Election Commission standards

Article 17. Periodic Review of Election Observer Panel Plans

Article 18. Definitions

Exhibit 1. Certificate of Biennial Inspection

Exhibit 2. Certification by Accuracy and Program Verification Board

Detailed Analysis

Article 1. Introduction

- 101. General Authority
- 102. Approval and Certification Required
- 103. Conditions for Approval and Certification
- 104. Rationale of Certification Process

Article 2. Jurisdiction

- 201. Reservation of Powers
- 202. Certificates of Inspection
- 203. Delegation of Powers

Article 3. Voting Systems and Procedures Panel, Advisory Committee, and Technical Consultants

- 301. Applicability of Procedure
- 302. Voting Systems and Procedures Panel
- 303. Composition of Voting Systems and Procedures Panel
- 304. Advisory Committee
- 305. Technical Consultants
- 306. Public Meetings

Article 4. Application for Approval and Certification

- 401. Who Can Apply For Approval And Certification
- 402. Time to Apply
- 403. Contents of Application
- 404. Application Complete Before Examination Begins
- 405. Voting Equipment to be Submitted
- 406. Demonstration of the Item Proposed for Approval or Certification
- 407. Deposit Required for Examination Costs

Article 5. Evaluating Applications

consulting

Gartner

Engagement: 220608071

© 2004 Gartner, Inc. and/or its affiliates.

For internal use of State of Arizona only.

All Rights Reserved.

—Page 11

- 501. Completeness of Application
- 502. Statement of Impact
- 503. Administrative Review and Preliminary Evaluation of Applications
- 504. Elements to Be Considered in the Review of an application
- 505. Applications Which Require Approval by the Voting Systems Panel
- 506. Applications Which Do Not Require Approval by the Voting Systems Panel
- 507. Approval May Be Conditioned
- 508. Decision in Writing
- 509. Decision Incorporated into Procedures, Guidelines, Other Materials
- 510. Appeal of Administrative Decision
- 511. Period for Appeal
- 512. Form of Appeal
- 513. Circulation Prior to Voting Systems Panel Hearing

Article 6. Criteria for Approval or Certification

- 601. Examination and Approval Criteria
- 602. Procedures for Use of the Proposed Item

Article 7. Examination and Testing

- 701. Examination and Testing
- 702. Examination and Testing of Voting Equipment
- 703. Mock Elections

Article 8. Modifications and Re-Examination

- 801. Re-Examination
- 802. Application Information for Examination
- 803. Contents of Application

Article 9. Public Hearing

- 901. Public Hearing
- 902. Time and Place of Hearing

consulting

Gartner

- 903. Cost of the Hearing
- 904. Agenda
- 905. Transcripts
- 906. Witnesses

Article 10. Decision of the Secretary of State

- 1001. Postponement of Decision
- 1002. Decision
- 1003. Approval Required Before Use
- 1004. New Application Permitted

Article 11. Periodic Review of Voting Systems

- 1101. Periodic Review of Approved Voting Systems
- 1102. Reasons for Periodic Review

Article 12. Decertification of Voting Systems and Vote Tabulating Systems

- 1201. Decertification
- 1202. Notice of Rescission
- 1203. Request for Reconsideration
- 1204. Public Hearing on Reconsideration

Article 13. Acceptance Testing

- 1301. Acceptance Testing
- 1302. Certify Results of Acceptance Testing
- 1303. Requirement for Corrections to Improper or Faulty Equipment
- 1304. Suspension of Certification

Article 14. Maintenance Logs

- 1401. Maintenance Logs
- 1402. Format of Maintenance Logs
- 1403. Suspension of Voting System

consulting

Gartner

Engagement: 220608071

© 2004 Gartner, Inc. and/or its affiliates.

For internal use of State of Arizona only.

All Rights Reserved.

—Page 13

1404. Reinstatement of Certification

Article 15. Biennial Tests of Voting Equipment

- 1501. Biennial Testing
- 1502. Certificate of Biennial Inspection
- 1503. Test Requirements
- 1504. Test Preparation
- 1505. Local Elections Officials' Responsibility
- 1506. Time of Submission of Certification

Article 16. Adoption of Federal Election Commission Standards

- 1601. FEC Standards Are Adopted

Article 17. Periodic Review of Election Observer Panel Plans

- 1701. Election Observer Panel Plan
- 1702. Periodic Review of Election Observer Panel Plans
- 1703. Model Election Observer Panel Plan

Article 18. Definitions

- 1801. Acceptance Test
- 1802. Accuracy
- 1803. Audit Trail
- 1804. Auditability
- 1805. Auxiliary Equipment
- 1806. Ballot
- 1807. Ballot Card
- 1808. Card Reader
- 1809. Certificate of Biennial Inspection
- 1810. Certification by Accuracy and Program Verification Board
- 1811. Certification Test Deck
- 1812. Certification Testing

consulting

Gartner

Engagement: 220608071

© 2004 Gartner, Inc. and/or its affiliates.

For internal use of State of Arizona only.

All Rights Reserved.

—Page 14

- 1813. Contest
- 1814. County and City
- 1815. Data Accuracy
- 1816. Data Integrity
- 1817. Data Security
- 1818. Demonstrator
- 1819. Direct Recording Electronic (DRE) Equipment
- 1820. Documentation
- 1821. Election
- 1822. Election Observer Panel Plan
- 1823. Elections Official
- 1824. Escrow
- 1825. Escrow Facility
- 1826. Examination or Review
- 1827. Functional Test
- 1828. Hardware
- 1829. Log of Maintenance Performance
- 1830. Maintenance Log
- 1831. Mark Sense Voting System
- 1832. Modification
- 1833. Modified Existing Systems
- 1834. Modified New Systems
- 1835. Operation Manual
- 1836. Party
- 1837. Pre-Audited Group of Ballots
- 1838. Printout
- 1839. Punch Card or Mark Sense Ballot
- 1840. Punch Card Voting System
- 1841. Qualification Testing
- 1842. Re-Certification
- 1843. Reliability
- 1844. Software

- 1845. Source Code
- 1846. Special Election
- 1847. Specific Environmental Conditions 1848. Test Deck
- 1849. User-Friendly
- 1850. Validation
- 1851. Vendor
- 1852. Verification
- 1853. Vote Tabulating Device
- 1854. Vote Tabulating Program
- 1855. Voting Device
- 1856. Voting Machine
- 1857. Voting Position
- 1858. Voting System

Exhibit 1. Certificate of Biennial Inspection

Exhibit 2. Certification by Accuracy and Program Verification Board

Procedures for Approving, Certifying, Reviewing, Modifying, and Decertifying Voting Systems, Vote Tabulating Systems, Election Observer Panel Plans, and Auxiliary Equipment, Materials, and Procedures.

Article 1. Introduction

101. General Authority

The Secretary of State, in exercising his or her statutory authority, has the duty to approve, certify, review, and decertify voting systems and vote tabulating systems [system], including specific models of a system, and to adopt procedures governing the approval, certification, review, decertification, and use of a system in accordance with the provisions of Division 19 of the California Elections Code (§§ 19001 and following). In the furtherance of open elections at each phase of the automated process of tabulating ballots, the Secretary of State requires that each election jurisdiction (county, city, city and county, district, etc.) prepare and submit for approval its plan to provide access to that portion of the elections process. These plans, called Election Observer Panel Plans, will be filed with the Secretary of State prior to the first use of the system and updated each time the environment in which they are used changes.

102. Approval and Certification Required

At any election, all or any portion of which is conducted under the authority of the Elections Code, votes shall be cast, registered, recorded, and counted by means of voting systems, procedures, and vote tabulating systems that have been approved and certified by the Secretary of State for use in California elections. Conversely, no voting system and no vote tabulating system, in whole or in part, shall be used in any election conducted under California law, unless the Secretary of State has approved and certified that system.

103. Conditions for Approval and Certification

(a) For any voting machine, voting device, vote tabulating device, and any software used for each, including the programs and procedures for vote tabulating and testing, or any modification to any of the above, to be certified for use in California elections, the criteria by which the Secretary of State evaluates such machine, procedure, device, modification, or software shall include, but not be limited to, the following:

- (1) The machine or device and its software shall be suitable for the purpose for which it is intended;
- (2) The system shall preserve the secrecy of the ballot;
- (3) The system shall be safe from fraud or manipulation;
- (4) The system shall be auditable for the purposes of an election recount or contest procedure; (5) The system shall comply with all appropriate federal and California laws and regulations, and;
- (6) The system shall have been certified, if applicable, by means of qualification testing by a Nationally Recognized Test Laboratory (NRTL) and shall meet or exceed the minimum requirements set forth in the Performance and Test Standards for Punch Card, Mark Sense, and Direct Recording Electronic Voting Systems, or in any successor voluntary standard document, developed and promulgated by the Federal Election Commission.

(b) In addition to the requirements of subdivision (a) of this section, voting systems, procedures, and equipment approved and certified by the Secretary of State shall promote accessible voting opportunities for persons with physical disabilities.

104. Rationale of Certification Process

(a) Certification consists of three separate levels of testing: qualification, certification and acceptance.

(b) Certification tests shall include functional tests and qualitative assessment to ensure that the system operates in a manner that is acceptable under federal and state law and regulations.

(c) Certification tests shall enhance public confidence by assuring that the system protects the secrecy of the ballot and the security of the voting process, and records and counts votes accurately.

(d) Certification tests shall promote public confidence that the system is easy to use or 'voter friendly.'

(e) Certification testing shall demonstrate that the system creates an audit trail showing both that the voter was able to vote for the candidate or for or against a measure of his or her choice and that the system correctly and consistently interpreted the voter's votes.

Article 2. Jurisdiction

201. Reservation of Powers

The Secretary of State reserves the right to approve, disapprove, certify, and decertify, as appropriate:

- (a) New or modified voting systems and vote tabulating devices;
- (b) New or modified procedures and regulations required for the use of such approved voting systems and vote tabulating devices;
- (c) New or modified Election Observer Panel Plans for each election jurisdiction conducting an election at which approved voting systems and vote tabulating devices are used, and;
- (d) The formats and specifications for ballots to be used with approved voting systems and vote tabulating devices.

202. Certificates of Inspection

The Secretary of State shall receive:

- (a) Not later than January 1 of every odd-numbered year:
 - (1) Certificates of Biennial Inspection from elections officials conducting any California election at which automated voting systems and vote tabulating devices are used. (See appended certificate);
 - (2) Certificates of Biennial Inspection from vendors who lease to, rent to, or allow elections officials to use any automated voting system or vote tabulating device in any California election. (See appended certificate)
- (b) Not less than seven days before any state election, including elections to fill vacancies, certificates from Accuracy and Program Verification Boards in each election jurisdiction in which automated voting systems are used. (See appended certificate)

203. Delegation of Powers

The Secretary of State may delegate duties to the Voting Systems and Procedures Panel:

- (a) To review periodically all approved voting systems, voting devices and vote tabulating devices, as well as the required regulations and procedures for their use, and to make recommendations to the Secretary of State regarding their continued approval for use in California elections;
- (b) To review periodically each election jurisdiction's approved Election Observer Panel Plans;
- (c) To review periodically all approved formats and specifications for ballots to be used with approved voting systems and vote tabulating devices;

(d) To review and make recommendations on applications for new voting and vote tabulating systems, equipment, materials, and procedures, as well as modifications to existing voting and vote tabulating systems, equipment, materials, and procedures, and;

(e) To establish an agenda and to conduct a public meeting for the purpose of reviewing applications and making recommendations to the Secretary of State.

Article 3. Voting Systems and Procedures Panel, Advisory Committee, and Technical Consultants

301. Applicability of Procedure

This procedure shall apply to all voting systems, voting devices, vote tabulating systems, equipment, materials, and procedures.

302. Voting Systems and Procedures Panel

The Secretary of State may establish a Voting Systems and Procedures Panel [Panel] to review proposed voting and vote tabulating systems, procedures, materials, and equipment, including proposed modifications, for certification and make recommendations to the Secretary of State regarding certification.

303. Composition of Voting Systems and Procedures Panel

The Secretary of State shall review the membership of the Panel, and may appoint members to it as needed. The appointed members shall serve at the pleasure of the Secretary of State. Panel members shall not hold or exercise any direct or indirect financial interest(s) in voting systems, vote tabulating systems, or any other equipment used with such systems.

304. Advisory Committee

The Secretary of State may also appoint membership to an advisory committee to assist the Secretary in evaluating voting systems, voting devices, vote tabulating systems, and any other issue or item to come before the Panel. The appointed members serve at the pleasure of the Secretary of State.

305. Technical Consultants

The Secretary of State may retain, as required, one or more technical consultants to conduct tests, review specifications, write reports, make recommendations, and otherwise assist the Secretary of State and the Panel. No consultant shall hold or exercise any direct or indirect financial interest(s) in voting systems, vote tabulating systems, or any other equipment used with such systems.

306. Public Meetings

The Secretary of State or his or her designee will convene panel meetings. The meetings shall be conducted publicly with appropriate notice and publication of the agenda. The Secretary of State's Elections Division will provide support staff.

Article 4. Application for Approval and Certification 401. Who Can Apply For Approval And Certification

Any person or corporation [applicant] owning or being interested in a voting system or a vote tabulating system, part of a system, equipment, materials or procedure may apply to the Secretary of State for approval or certification.

402. Time to Apply

The applicant may apply to the Secretary of State at any time. 403. Contents of Application

The application shall be in writing, on a form supplied by the Secretary of State, and shall include at least the following information:

- (a) Information about the applicant, including name, address, telephone number, and business address, if applicable;
- (b) Complete and detailed description of the item(s) or procedures to be approved or certified, including whether the application is for a new item or for modification of an existing item;
- (c) Information about the product or procedure that is being reviewed, including, but not limited to, version numbers, release numbers, operating and maintenance manuals, training materials, technical and operational specifications, installed customer lists, photographs, promotional materials, etc;
- (d) Reports for all tests conducted on the item being reviewed for approval or certification by any Nationally Recognized Test Laboratory (NRTL);
- (e) Documentation that the item meets the Federal Election Commission Voting Equipment guidelines;
- (f) The applicant is encouraged to include certification documents from other states that have certified the equipment;
- (g) A list of other states, counties, and municipalities where the system is presently in use;
- (h) A list of other states, counties, and municipalities where the system has been used but is no longer in use;
- (i) A list of any other states where an application has been made for approval of the equipment, and a statement as to whether the equipment was approved, disapproved, or the application is pending;

(j) Information describing any financial relationship between the applicant and the manufacturer, distributor, or retailer of the various components of the equipment for which approval is sought, and; (k) Other information or materials the applicant wishes to provide;

The Secretary of State may request additional information from the applicant.

404. Application Complete Before Examination Begins

Only after the Secretary of State has received a completed application from the applicant may an examination begin. No application shall be deemed to be complete until all documentation and fees required by these procedures has been submitted to the Secretary of State or his or her designee.

405. Voting Equipment to be Submitted

(a) The applicant shall make a working model of the item under review available to the Secretary of State for the duration of the review.

(b) The Secretary of State may require the applicant to cover the expenses of one or more Nationally Recognized Test Laboratory (NRTL), laboratory, and/or technical experts to assist in examining the item.

(c) The equipment for which approval is sought shall be made available for examination and certification testing for a period of at least 30 days before the equipment's public hearing by the Voting Systems and Procedures Panel.

(d) Any operating systems or programs accompanying the equipment shall be designed to count votes accurately.

(e) The format of the test ballots presented with the equipment shall be for an actual primary election and an actual general election.

(f) The applicant shall provide necessary ballot cards and other pertinent materials and equipment in sufficient quantity to test the equipment extensively.

(g) The applicant shall provide the Secretary of State with instruction information and all available specifications.

406. Demonstration of the Item Proposed for Approval or Certification

The Secretary of State shall require that the applicant demonstrate the proposed system, equipment, procedure, or materials to the Secretary of State or his or her designee.

407. Deposit Required for Examination Costs

The Secretary of State may require the applicant submitting the equipment to deposit moneys into an Agency Trust Account sufficient to guarantee and reimburse the cost of any contract for consultation or any other costs associated with the examination of a proposed item.

Article 5. Evaluating Applications

501. Completeness of Application

Upon receipt of an application, the Secretary of State shall examine the application for completeness. If the application is not complete, the Secretary of State shall notify the applicant of the information required to complete the application. No application will be considered for approval or certification unless it is complete, including all required fees.

502. Statement of Impact

The Secretary of State, based on the materials provided with the application, shall produce a statement summarizing the application and its impacts or effects on voting in California.

503. Administrative Review and Preliminary Evaluation of Applications

Once an application is complete, the Elections Division of the Secretary of State's office shall, within 30 days, conduct an administrative review of the application and will provide recommendations to the Secretary of State as to whether the application requires a meeting of the Voting Systems Panel or if it can be approved or rejected administratively.

504. Elements to Be Considered in the Review of an application

Upon receipt of a completed application, the Secretary of State shall evaluate the application. This evaluation shall include, but is not necessarily limited to:

- (a) A review of California Elections Code sections which address the application;
- (b) A review of federal statutes or regulations which address the application;
- (c) A copy of the approved Qualification Test results released directly to the Secretary of State by a Nationally Approved Test Laboratory (NRTL).
- (d) A review, if applicable, of transcripts or other materials from prior meetings or hearings on the proposed system, procedure, or modification either in whole or in part;
- (e) A review, if applicable, of any procedures manuals, guidelines or other materials adopted for use with the system addressed by the application;
- (f) A review of any effect the application will have on the security of the election system;
- (g) A review of any effect the application will have on the accuracy of the election system;
- (h) A review of any effect the application will have on the ease and convenience with which voters use the system;
- (i) A review of any effect the application will have on the timeliness of vote reporting, and,

(j) A review of any effect the application will have on the overall efficiency of the election system.

(k) A Description of Deposit Materials showing that the Ballot Tally Software Source Code has been deposited in Escrow with an Escrow Company approved pursuant to Chapter 6, Division 7, Title 2 of the California Administrative Code, beginning with Section 20630.

505. Applications That Require Approval by the Voting Systems Panel

The Voting Systems Panel shall review any application that is determined to affect materially the security of elections, the accuracy of voting or vote counting, convenience to the voter, lawful conduct of elections, the integrity of the elections process, or otherwise result in significant modification to existing procedures.

506. Applications That Do Not Require Approval by the Voting Systems Panel

Any application that the Secretary of State determines does not materially affect the lawful conduct, accuracy, or security of elections, or which does not materially affect the convenience to the voter of the elections process, may be approved administratively.

507. Approval May Be Conditioned

Any approval may contain additional requirements of one or more actions or procedures, as determined by the review of the application.

508. Decision in Writing

Any decision to approve, certify, decertify, modify, or otherwise respond to an application shall be in writing under signature of the Secretary of State and shall include a statement of reasons for the decision with specific reference to each of the criteria identified in § 504 above.

509. Decision Incorporated into Procedures, Guidelines, Other Materials

Within 30 days the applicant shall incorporate and submit to the Secretary of State for approval all the recommendations required by the Secretary of State for certification for inclusion into all appropriate procedures, guidelines, and other materials affected by the application.

510. Appeal of Administrative Decision

An applicant may appeal any administrative decision to the Secretary of State within 30 days of receipt of the written decision. The appeal shall be made on a form provided by the Secretary of State.

511. Circulation Prior to Voting Systems Panel Hearing

At least 30 days prior to a meeting of the Voting Systems Panel to consider an application, a notice of the proposed changes shall be circulated to all interested parties.

Article 6. Criteria for Approval or Certification 601. Examination and Approval Criteria.

The Secretary of State shall not approve a proposed item without a finding that the item conforms to all applicable laws, procedures and regulations, including the right to a secret ballot, does not compromise the accuracy, security or integrity of the election process, nor interferes with the voter's ease and convenience in voting.

602. Procedures for Use of the Proposed Item

Approval or certification of a proposed item by the Secretary of State shall not take effect until all applicable procedures for its use have been formulated, approved, and incorporated into the appropriate documentary records. Final approval or certification will include a condition that the contract of sale shall provide that the equipment will work properly under provisions of California election laws, rules and regulation and that the procedures formulated for its operation have been approved by the Secretary of State. A copy of the procedures shall be submitted by the applicant or vendor to a prospective purchaser.

Article 7. Examination and Testing 701. Examination and Testing

The Secretary of State shall conduct, as appropriate, tests and examinations of the proposed item to ensure that it meets the criteria for approval or certification. Examination and testing may consist of one or more functional application tests designed to ensure that the system or equipment meets all applicable procedures, regulations, guidelines and laws, and may include examination or testing by technical experts, including an Nationally Recognized Test Laboratory (NRTL) or laboratory.

702. Examination and Testing of Voting Equipment

All equipment proposed to be used for elections in California shall be examined and tested to ensure proper and accurate operation. The examination and testing shall include, but not be limited to, the set-up and conduct of at least two mock elections. The applicant shall provide ballot materials and programming to create these elections.

703. Mock Elections

(a) The equipment shall be examined and tested by conducting a mock presidential primary, as defined by California law, and shall to verify, among other things, the provisions for, and the results of, each presidential primary election and the rotation of candidate names for partisan and non-partisan offices, as necessary.

(b) The equipment shall be examined and tested in conducting a mock gubernatorial general election in order to test the rotation of candidate names for any office, as well as the results of a state and two local recall elections.

(c) Both mock elections shall feature at least ten precincts with at least ten ballots in each precinct, representing ballots cast at the precinct. Five additional ballots shall represent absent voter ballots.

(d) In the case of the mock primary election, each qualified political party eligible to participate in the primary shall be represented by at least ten ballots in each precinct. Five additional ballots for each eligible party shall represent absent voter ballots. At the time the equipment is presented for examination and approval, the applicant should verify the number and names of the qualified political parties and should ascertain and follow any laws affecting the counting of partisan ballots at primary, special and general elections, and the rules affecting recall elections. The requirements of this section may be modified to accommodate a “blanket” primary election, if necessary.

Article 8. Modifications and Re-Examination

801. Re-Examination

Any modification, change, or other alteration to a voting or vote tabulating material, equipment, component or procedure shall require approval or certification before it may be used in California elections.

802. Application Information for Examination

An applicant may apply to the Secretary of State for the review of a modification of an existing certified system at any time during the year. Evaluation of the need for re-certification or examination will occur at the convenience and judgment of the Secretary of State. Application, examination, and testing of proposed modifications shall be done according to the same procedures as applications for new items.

803. Contents of Application

In addition to the information required in section 403, an application for modification of an existing voting or vote tabulating system, equipment, material, or procedure shall provide a description, in complete operational and technical detail, of all differences between the originally certified equipment, material, procedure or system and the proposed modification.

Article 9. Public Hearing

901. Public Hearing

The Secretary of State shall schedule a public hearing for any item requiring Panel consideration. The purpose of the hearing shall be to receive testimony and information on proposed systems,

materials, equipment or procedures, as well as modification to systems, materials, equipment and procedures. At the hearing, the applicant may be expected to conduct a demonstration and explain the application, as well as to answer questions from the Panel. The applicant may be asked to submit answers in writing if the Secretary of State is not satisfied with the completeness of answers given at the hearing.

902. Time and Place of Hearing

Hearings will be scheduled from time to time by the Secretary of State. Unless otherwise announced, hearings will be held at the Secretary of State's Office, 1500 Eleventh Street, Sacramento, California 95814.

903. Cost of the Hearing

The cost of the hearing will be borne by the State

904. Agenda

A copy of the agenda, including any amendments, will be available to all persons in attendance, and will be provided to all interested parties not less than 30 days in advance of the hearing..

905. Transcripts

Hearings will be stenographically recorded. Copies of the transcript may be purchased from the court reporter, or obtained from the Secretary of State, approximately three weeks after the hearing. The charge for the copy from the Secretary of State shall be in accord with statutory provisions in effect at the time the request for the copy is made.

906. Witnesses

Applicants may arrange for witnesses and expert testimony in support of an application. Opponents of an application may also arrange for witnesses and expert testimony. Testimony or information may be provided in writing prior to or at the time of a hearing.

Article 10. Decision of the Secretary of State

1001. Decision

The decision of the Secretary of State, either approving, disapproving, or withholding approval of a voting machine, voting device, vote tabulating device, material, equipment, or procedure shall be made in writing, to the applicant, within 30 days of the hearing or provision of additional written materials as specified in Section 1002 (below). The decision shall state whether the system,

consulting

Gartner

equipment, material, or procedure so examined complies with the requirements of California election laws and regulations and can be safely used by voters at elections under the conditions prescribed in California election laws and regulations. The decision shall be filed with the Secretary of State, shall be reported to the Governor and Attorney General, shall be open to public inspection and, within 40 days from the date of the hearing, copies shall be sent to the county boards of supervisors, county and municipal elections officials, vendors of elections services and supplies, and interested parties.

1002. Postponement of Decision

The Secretary of State may postpone his or her decision, pending receipt of additional written information, testimony, or examination of materials.

1003. Approval Required Before Use

No system, material, equipment, or procedure, in whole or part, may be used in elections in California unless it has received the approval of and been certified for use by the Secretary of State.

1004. New Application Permitted

Denial of an application shall not prevent the applicant from submitting a new application to the Secretary of State.

Article 11. Periodic Review of Voting Systems 1101. Periodic Review of Approved Voting Systems

Pursuant to Elections Code 19222, the Secretary of State shall periodically review voting systems to determine whether they are defective, obsolete, or otherwise unacceptable. After such review, approval previously granted may be withdrawn. Six months notice must be given prior to withdrawing approval of any voting system unless the Secretary of State shows good cause for a shorter notification period. Any withdrawal by the Secretary of State of his or her approval of a voting system or part of a voting system shall not be effective as to any election conducted within six months of that withdrawal.

1102. Reasons for Periodic Review

The periodic review shall examine certified voting systems and evaluate alternative systems to assure that elections are conducted so as to:

- (a) Protect the secrecy of the ballot;
- (b) Protect the security of the voting process; (c) Record and count votes accurately; and,
- (d) Comply with all pertinent election laws, regulations, and procedures.

Article 12. Decertification of Voting Systems and Vote Tabulating Systems 1201. Decertification

If, at any time after the Secretary of State has certified a voting system, he or she determines that the voting system fails to meet the standards set forth in California election law, and upon

consideration of the criteria required by the Examination Criteria section of these procedures, the Secretary of State shall notify any users and vendors of that particular voting system that the certification of that system for future use and sale in California is to be withdrawn.

1202. Notice of Rescission

The notice shall be in writing and shall specify the reasons why the certification of the system is being rescinded and the date on which the decertification is to become effective.

1203. Request for Reconsideration

An applicant or user of that voting system may request in writing that the Secretary of State reconsider its decision to decertify the voting system.

1204. Public Hearing on Reconsideration

Upon receipt of the request to reconsider, the Secretary of State shall hold a public hearing for the purpose of reconsidering the decision to decertify the voting system. Any interested party shall be given the opportunity to submit testimony or documentation in support of, or in opposition to, the Secretary of State's decision to decertify that particular voting system. Following the hearing, the Secretary of State may affirm or reverse his or her decision.

Article 13. Acceptance Testing

1301. Acceptance Testing

(a) Whenever an election jurisdiction acquires a new system or modifies an existing system previously certified by the Secretary of State, the election jurisdiction must perform acceptance tests of the equipment before it may be used to cast or count votes at any election. The equipment must be operating correctly, pass all tests, and must be identical to the equipment certified by the Secretary of State.

(b) The vendor must provide all manuals and training necessary for the proper operation of the system.

(c) The election jurisdiction shall perform a series of functional and programming tests that will test all functions of the ballot counting system. This must include processing a substantial number of test ballots of various pre-punch or ballot codes, including split precincts, rotated races, multiple candidates, cumulative reports, precinct reports, canvass reports, and any other tests the election jurisdiction authority finds necessary.

1302. Certify Results of Acceptance Testing

The results of acceptance testing shall be certified to the Secretary of State.

1303. Requirement for Corrections to Improper or Faulty Equipment

If the acceptance test reveals any improper or faulty voting systems equipment, the applicant must make corrections to such improper or faulty equipment within 30 days from the date of such acceptance testing, or as otherwise provided for by contract.

1304. Suspension of Certification

The Secretary of State, upon his or her review of the acceptance testing of such equipment may, at his or her discretion, suspend certification of said equipment for future sales in the State of California, in accordance with the Rescission of Certification provisions of these procedures. Such certification may be reinstated after a complete review of further testing.

Article 14. Maintenance Logs

1401. Maintenance Logs

Each election jurisdiction and voting supplies vendor which has purchased voting systems equipment shall keep a detailed log of maintenance, performance and testing procedures for each piece of such equipment in its inventory.

1402. Format of Maintenance Logs

Such logs shall be in a format specified by the Secretary of State, which shall be reviewed by the applicant, and which shall be available for periodic review and inspection by the Secretary of State.

1403. Suspension of Voting System

The Secretary of State may, after a hearing, suspend the use of any voting system or component thereof in any election jurisdiction in which proper maintenance procedures or proper servicing by the manufacturer have not been fully implemented.

1404. Reinstatement of Certification

The Secretary of State may reinstate the certification based upon review of these procedures and a review of the maintenance logs.

Article 15. Biennial Tests of Voting Equipment 1501. Biennial Testing

A biennial test of electronic or computerized voting equipment shall be conducted on each piece of equipment under the jurisdiction of any elections official or vendor of election services.

1502. Certificate of Biennial Inspection

Certificate of Biennial Inspection means a certification, required by Elections Code § 19220, stating that all voting and vote counting equipment has been examined by the appropriate elections official before its use in an election and has been found to be operating correctly and accurately.

1503. Test Requirements

For a centralized vote county system, biennial testing shall include, at a minimum, 800 votes.

1504. Test Preparation

Such tests shall be prepared by the local elections official or voting supplies vendor.

1505. Local Elections Officials Responsibility

The local elections official shall certify to the Secretary of State that the testing of each piece of equipment within its jurisdiction has been completed. Such certification shall be on a form prescribed by and furnished by the Secretary of State.

1506. Time of Submission of Certification

The test certification shall be submitted to the Secretary of State not less than seven days before an election.

Article 16. Adoption of Federal Election Commission Standards 1601. FEC Standards are Adopted

The Federal Election Commission standards concerning voting systems and software escrow are hereby included by reference, except where otherwise modified by federal and California laws and regulations.

Article 17. Periodic Review of Election Observer Panel Plans 1701. Election Observer Panel Plan

Each county election official shall prepare an Election Observer Panel Plan. This plan shall provide for meaningful public observation of the vote counting process, and shall be filed not later than January 15th of each even-numbered year with the Secretary of State.

1702. Periodic Review of Election Observer Panel Plans

The Secretary of State shall review Election Observer Panel Plans for each county and shall provide comment, as necessary, by February 15th of each even-numbered year.

1703. Model Election Observer Panel Plan

The Secretary of State shall develop, and distribute to each county election official, a model Election Observer Panel Plan.

Article 18. Definitions

1801. Acceptance Test means the examination of voting systems and their components by the purchasing election authority in a simulated use environment to validate performance of delivered units in accordance with procurement requirements; testing to validate performance may be less broad than that involved with qualification testing and successful performance for multiple units (precinct count systems) may be inferred from a sample test.

1802. Accuracy means precision in calculations and outputs.

1803. Audit Trail means a record of the manual and computing processes which have been applied to an election, showing each stage of processing and allowing the original data to be reconstituted. It permits verification of the integrity and reliability of the vote tabulating process as well as detection and correction of problems. A combination of manual and computer-generated documentation provides a record of each step taken in:

- defining and producing ballots and generating related software for specific elections;
- installing ballots and software;
- testing system readiness;
- casting and tabulating ballots; and,
- producing reports of vote totals.

The record incorporates system status and error messages generated during election processing, including a log of machine activities and routine and unusual intervention by authorized and unauthorized individuals. The audit trail also documents such items as ballots delivered and collected, administrative procedures for system security, pre-election testing of voting systems, and maintenance performed on voting equipment.

1804. Auditability means the ease of auditing the vote tabulating software, the ballots, and the canvass.

1805. Auxiliary Equipment means an independent component having a life of its own that is incorporated into the voting system, such as a card reader, printer or modem. It is not a permanent or enclosed part of the voting system.

1806. Ballot means a document on which the names of the candidates are printed for party positions or public office or contains ballot applications and on which the voter records his or her selection. A ballot may be comprised of two or more standard computer tabulating cards joined together which may be separated for the purpose of counting votes. (Cf. Elec C § 301)

1807. Ballot Card means the standard computer tabulating card produced when the stub has been removed from the ballot and when the full ballot, if necessary, has been separated into its sections. In these procedures, the term “ballot card” and “ballot” are sometimes used interchangeably. (Cf. Elec C § 302)

1808. Card Reader means a peripheral device for computers, used to read the data from ballot cards.

1809. Certificate of Biennial Inspection means a certification, required by § 19220, stating that all voting and vote counting equipment has been examined by the appropriate elections official before its use in an election and has been found to be operating correctly and accurately. (See appended certificate)

1810. Certification by Accuracy and Program Verification Board, sometimes known as Logic and Accuracy Board, means a certification, adopted pursuant to Elections Code § 19205, whereby any county, city and county, city, or district which uses a vote tabulating device, certifies that they have conducted their pre-vote counting tests, and made any necessary corrections to the test materials, at least seven days before the day of the election. (See attached sample form)

1811. Certification Test Deck means a pre-audited group of ballots voted with a pre-determined number of valid votes for each candidate, each write-in position and each voting position as a measure or proposition that appears on the ballot. It also includes one or more ballots that have been improperly voted or which are voted in excess of the number allowed by law in order to test the ability of the system to reject the votes, and one or more blank ballots.

1812. Certification Testing means the examination, and possibly testing, of a voting system to determine its compliance with state counting law and rules and any other state requirements for voting systems.

1813. Contest means the aggregate of candidates who run against each other or among themselves for a particular office. There must be a write-in voting square for each position to be filled in the contest. The positive and negative voting options of a ballot measure submitted to voters (Yes or No) also constitute a contest.

1814. County and City both include “city and county.” (Elec C § 310)

1815. Data Accuracy means the system's ability to process voting data without errors generated by the system internally. It is distinguished from data integrity which encompasses errors introduced by an outside source.

1816. Data Integrity means the invulnerability of the system to accidental intervention or deliberate, fraudulent manipulation that would result in errors in the processing of voting data. It is distinguished from data accuracy which encompasses internal, system generated errors.

1817. Data Security means the various methods and procedures, such as the use of passwords and encryption, implemented to prevent unauthorized use, destruction, or disclosure of data, whether it is accidental or deliberate.

1818. Demonstrator means a model or facsimile of the voting device or the portion of the face of a voting machine that shows the voter how to operate the machine. (Elec C § 315)

1819. Direct Recording Electronic (DRE) Equipment means an electronic voting machine (q.v.).

1820. Documentation means facts, manuals, notes, or instructions which are used to explain system functionality, software and hardware characteristics, and developmental testing.

1821. Election means any election including a primary that is provided for under the Elections Code. (Cf. Elec C § 318)

1822. Election Observer Panel Plan means a plan filed with the Secretary of State by any election jurisdiction (county, city and county, city, district) which counts its voted ballots at a place other than the precinct at which the ballots were cast, or uses a vote counting device to count and summarize its voted ballots. The purpose of the plan is to maintain the integrity of the public vote counting required by § 15054.

1823. Elections Official means any of the following:

(a) A clerk or any person not covered by sub-section (b) who is charged with the duty of conducting an election.

(b) A county clerk, registrar of voters, city clerk, elections supervisor, or governing board having jurisdiction over elections within any county, city, or district within the state. (Cf. Elec C § 320)

1824. Escrow means the process by which a third party having no direct or indirect financial interest with a vendor holds, for safekeeping and possible verification, the voting system software source code, including all changes or modifications and new or amended versions. A financial interest would exist if the third party, for instance, included a vendor's stocks in its portfolio.

1825. Escrow Facility means the physical location in which the source code may be stored. No election jurisdiction may act as an escrow facility.

1826. Examination or Review means the inspection or analysis by a test authority, state certification authority, or local jurisdiction of the system hardware, software and other system documentation, test documentation, or documentation of modifications to ascertain if the system complies with the standards, state code, or procurement contract requirements and to determine if further testing is required.

1827. Functional Test means an empirical test performed to verify or validate the accomplishment of a function or a series of functions.

1828. Hardware means the mechanical, electrical and electronic assemblies, including materials and supplies, which are a part of the voting system, such as microprocessor (CPU), I/O devices, printer, circuit boards, integrated circuits, and power supply. Hardware includes the voting device on which individual voters cast their ballot, as well as the actual equipment which is used to program ballot software or central vote tabulation software.

1829. Log of Maintenance Performance means a written record which contains all information relating to performance of scheduled and non-scheduled maintenance requirements recommended by the vendor or manufacturer of such equipment and all service visits performed by vendor or manufacturer.

1830. Maintenance Log means a written record which contains all information relating to system testing, performance of scheduled and non-scheduled maintenance requirements recommended by the vendor or manufacturer of such equipment, and all service visits performed by vendor or manufacturer.

1831. Mark Sense Voting System means a system by which votes are recorded by means of marks made in voting response fields designated on one or both faces of a ballot card or series of cards.

1832. Modification means any change in either software, firmware, hardware, or procedure for use that directly affects the operation of the voting system that will require reexamination of certified equipment by the Secretary of State.

1833. Modified Existing Systems mean existing systems that have been modified to be in partial or full compliance with the performance and design standards.

1834. Modified New Systems mean voting systems previously developed tested in compliance with the standards and that are subsequently modified.

1835. Operation Manual means (1) a manual of all procedures used to prepare the equipment and provide proper maintenance procedures, including the unpacking and storage procedures to be used by local elections officials, and (2) a manual of election day set-up and election day operating procedures to be used by local elections officials.

1836. Party means a political party or organization that has qualified for participating in any primary election. (Elec C § 338)

1837. Pre-Audited Group of Ballots means a test deck whose contents are known.

1838. Printout means the printed copy of (1) zero totals, candidate names and offices and other information produced by the counting equipment prior to the official canvass of the ballots and (2) the ballots cast for each candidate and question, the names of candidates and the offices for each candidate and other information provided after the official ballot tabulation.

1839. Punch Card or Mark Sense Ballot means a tabulating card on which the voter may record his or her vote by punching or marking at designated locations on the card. (Cf. Elec C § 344)

1840. Punch Card Voting System means one where votes are recorded by means of punches made in voting response fields designated on one or both faces of a ballot card or series of cards.

1841. Qualification Testing means the examination and testing of a computerized voting system by an independent test authority using FEC test standards to determine if the system complies with the FEC performance and design standards. This process occurs before certification testing.

1842. Re-Certification means the examination, and possibly the retesting, of a voting system which was modified after having been certified for use in California elections. The object of this process is to determine if the modification still permits the system to function in accordance with state requirements.

1843. Reliability means the probability that an item will perform a required function, under stated conditions, for a stated period of time. Reliability is therefore the extension of quality into the time domain and may be paraphrased as ‘the probability of non-failure in a given time.’

1844. Software means the application and operating system programs associated with a computer, as opposed to hardware that refers to the physical components of a computer system. Software means any and all codes for operation of the vote counting system including ballot tabulation system bootstrap, monitor and device controllers, operating system, ballot layout, system audit and report generation. Software includes all programs, voting devices, cards, ballot cards or papers, operating manuals or instructions, test procedures, printouts, and other non-mechanical or non-electrical items necessary to the operation of a voting system. (Cf. Elec C § 355)

1845. Source Code means the specific language a programmer uses to program the electronic equipment or vote tabulating system. The source code of the computer language is then compiled, interpreted, or assembled into object code by the computer. The result is a machine language program in binary form which can be run by the computer.

1846. Special Election is an election, the specific time for the holding of which is not prescribed by law. (Elec C § 356)

1847. Specific Environmental Conditions means and shall include the effect of natural environmental conditions such as temperature, humidity and dust, and induced environmental conditions such as handling, storage or transportation which may affect the operation of the equipment.

1848. Test Deck means a pre-audited group of ballots voted with a pre-determined number of valid votes for each candidate, each write-in position and each voting option on a question or proposition that appears on the ballot. It also includes one or more ballots that have been improperly voted or which are voted in excess of the number allowed by law in order to test the ability of the system to reject those votes, one or more blank ballots, and one or more ballots on which two or more votes are cast for a candidate whose name appears on the ballot more than once for the same office, in order to test the ability of the system to count only the first of such votes for the candidate.

1849. User-Friendly means a process or system which is easy to use and difficult to misuse.

1850. Validation means a test to find errors by executing a program in a real environment (i.e., during acceptance tests).

1851. Vendor means any manufacturer, company, or individual who seeks to sell, or sells, a voting system or a vote tabulating system for use in California elections.

1852. Verification means a test to find errors by executing a program in a simulated environment (i.e., during system qualification testing).

1853. Vote Tabulating Device means any piece of equipment, other than a voting machine, that compiles a total of votes cast by means of ballot card sorting, ballot card reading or scanning, paper ballot scanning, electronic data processing, or a combination of such equipment. (Elec C § 358) Examples: Documentation (IBM, Data General, etc.) Card Reader, PROM-PAK, etc.

1854. Vote Tabulating Program means the computer programs used for counting of votes cast on Ballots. It includes both any and all vendor software, and the coding programs specific to each election.

1855. Voting Device means any device used in conjunction with a ballot card or cards to indicate the choice of the voter by marking, punching, or slotting the ballot card. (Elec C § 360) Examples: Vote Recorder, Stylus.

1856. Voting Machine means any device upon which a voter may register his or her vote, and which, by means of counters, embossing, or printouts, furnishes a total of the number of votes cast for each candidate or measure. (Elec C § 361) Examples: Automatic (AVM), Shoup.

1857. Voting Position or Voting Square means an area or square or defined location on the ballot to the right of the candidate's name or ballot measure in which a punch or mark can be made to indicate a valid vote.

1858. Voting System means any mechanical, electro-mechanical, or electronic system and its software, or any combination of such used to cast or to tabulate votes, or both. (Elec C § 362)
Examples: DataVote, Mark-a-Vote, Votomatic; Pollstar, Optech, etc.

(Form Date is January 1997)

Certificate of Biennial Inspection State of California)

(City and) County of)

I, _____, Registrar of Voters/County Clerk of the (City and) County of _____, do hereby certify that in the normal course of pre-election hardware maintenance and testing of our voting and vote tabulating equipment for the forthcoming election on _____, I find that the voting and vote tabulating equipment used in said (City and) County is operating correctly and accurately. This Certificate is issued pursuant to Elections Code Section 19220.

Dated: (date)

Signed: (name and title)

[Seal]

(Form Date is January 1997)

Certification by Accuracy and Program Verification Board

State of California)

(City and) County of)

We, the undersigned members of the Accuracy and Program Verification Board, having been duly appointed by

_____, the Registrar of Voters/County Clerk of the (City and) County of _____, for the election to be held on _____, to verify the logic and accuracy test ballots as required by the Procedures for the use of the _____ System, adopted pursuant to Elections Code section 19205, do hereby certify through the Registrar of Voters/County Clerk to the Secretary of State:

THAT the pre-vote counting tests, as defined in the above-mentioned procedures, have been performed;

consulting

Gartner

Engagement: 220608071

© 2004 Gartner, Inc. and/or its affiliates.

For internal use of State of Arizona only.

All Rights Reserved.

—Page 36

THAT the pre-vote counting test results have been compared with the predetermined correct totals for each office and ballot measure;

THAT the cause of any discrepancy was found and corrected; and,

THAT the logic and accuracy test programs, the logic and accuracy test ballot cards, and the logic and accuracy test printed output which were certified as correct by the Accuracy and Program Verification Board were delivered into the custody of the Registrar of Voters/County Clerk.

We declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

SIGNATURE of First Board Member Date

PRINTED Name of First Board Member

SIGNATURE of Second Board Member Date

PRINTED Name of Second Board Member

SIGNATURE of Third Board Member Date

PRINTED Name of Third Board Member

(Insert as many signature blocks as there are board members)

Appendix E: State of Louisiana Certification Procedures

Introduction

After a major scandal concerning voting machine selection and procurement in the 1990s, Louisiana reformed its election management. The Division of Elections and Registration, created by legislature as part of a new state constitution in 1975, was placed under the Office of the Secretary of State by Act 451. The voters of Louisiana elected Suzanne Haik-Terrell as the new Commission of Elections in 1999. Terrell and the legislator significantly changed the processes to the certify, select, and procure voting systems.

While many states have had to invest heavily in updating voter registration, Louisiana's existing centralized database is substantially in compliance with the letter and spirit of the Help American Vote Act. Consequently, the state has been able to focus on obtaining new voting systems. One of the accomplishments of the office was a definitive description of voting system requirements. The "Voting System Certification Standards" was included in the Louisiana Help America Vote Act State Plan.

STATE OF LOUISIANA DEPARTMENT OF ELECTIONS AND REGISTRATION VOTING SYSTEM CERTIFICATION STANDARDS

Pursuant to La. R.S. 18:1351, any voting system proposed or bid for use in the State of Louisiana must meet or exceed the following standards. These standards include statutory standards found in La. R.S. 18:1355. These standards further include requirements established by the Commissioner of Elections pursuant to her authority under La. R.S. 18:1353.

The voting system must:

GENERAL REQUIREMENTS:

- ❑ Allow person to vote for or against, yes or no to, each question that is submitted;
- ❑ Permit the voter to vote for as many persons for an office as he is lawfully entitled to vote, but no more. However, where the voter may vote for more than one person for an office, it shall count each vote cast, even though the voter has voted for fewer than the total number of votes he is entitled to cast for a particular election;
- ❑ Permit the voter to vote for or against any question or race for which he has a right to vote, but no other;
- ❑ When used in a primary election at which members of a political party committee are to be voted on, it shall be so equipped that the election officials can lock out all candidate counters except those of the party with which the voter is affiliated;
- ❑ Correctly register and record and accurately count all votes cast for each candidate and for or against each question;
- ❑ Meet or exceed standards established by NASED and tested through Independent Testing Authorities;

- ❑ Have at least 250 voting positions with ability to expand to at least 500 positions;
- ❑ Have an internal real time clock that works in conjunction with all printouts and voting machine diagnostics performed for maintenance or operation purposes;
- ❑ Maintain all vote totals, public counter totals, audit trail records, protective counter totals and the internal clock time in both the main memory and the removable programmable memory devices in the event the main power and battery backup power fail;
- ❑ Be able to withstand a maximum temperature of 130 degrees Fahrenheit, while in storage, and 105 degrees Fahrenheit while in operation, and a minimum temperature of –15 degrees Fahrenheit, while in storage, and 40 degrees Fahrenheit, while in operation, without any permanent damage, degraded reliability or performance deterioration;
- ❑ Be able to survive exposure to uncontrolled temperature and non-condensing humidity environments, while in storage, and shall operate without damage to the component parts when operated at non-condensing relative humidity of up to 98%;
- ❑ Be designed so that no failure, short of destruction of the voting machine and programmable memory device, can result in the loss of vote counts or inaccurate vote counts;
- ❑ Provide printed records regarding the opening and closing of the polls, including:
 - ✓ Identification of election;
 - ✓ Identification of each unit;
 - ✓ Identification of ballot format;
 - ✓ Identification of candidate and/or issue, verifying zero start;
 - ✓ Identification of all ballot fields and all special voting options;
 - ✓ Summary report of votes cast for each device, or ability to extract same;
- ❑ Prevent printing of summary reports before the sequence of events required for closing of the polls are completed;
- ❑ Opening the polls reports should have all system audit information required;
- ❑ No data should be lost during generation of reports;
- ❑ Integrity and security of data maintained according to time frame for federal, state and local elections;
- ❑ Prevent unauthorized functions in an improper sequence;
- ❑ Include security provisions compatible with administrative set up and operational use;
- ❑ Allow for extraction of data from memory devices via land lines;
- ❑ Prevent loss of results, images and inaccurate vote count;
- ❑ Provide security procedures system-wide, from turn on to turn off;
- ❑ Prevent tampering or destruction of information through the introduction of a magnetic device;
- ❑ Provide for safeguards against tampering, theft or damage;
- ❑ Ensure that test data has been purged from the system;

SECURITY:

- ❑ Provide secrecy in the act of voting such that the selection of a voter cannot be determined after that vote has been cast;
- ❑ Prevent the voter from voting more than once on the same candidate race or on the same question;
- ❑ Permit all unused vote indicators or devices to be locked out against use;
- ❑ Provide a protective counter or tabulator;
- ❑ Provide a public counter or tabulator that at all times during the election shall show the number of persons who have voted;
- ❑ Contain one or more automatic locks that upon exposure of the vote count at any time after the polls are opened on election day will automatically lock the machine against further operation;
- ❑ Provide a screen, hood, or curtain that is so made and can be so adjusted as to conceal the voter while voting;
- ❑ Be incapable of being reset, altered, or used except by operating the machine;
- ❑ Provide for protective counter that advances each time the system reset is performed;

PROGRAMMING:

Contain for election for president and vice president, those devices needed in order to comply with R.S. 18:1259 (A copy of R.S. 18:1259 is attached as Appendix "1");

- ❑ Provide screen size, display and programming that shall be capable of producing a ballot of font sizes no less than 14 to 18 points in the following denominations:
 - ✓ Heading for races and propositions (18 points)
 - ✓ Names of candidates (16 points)
 - ✓ All other text, including text of propositions (14 points);
- ❑ Accommodate up to twelve (12) different parties or districts or combination of both within a precinct;
- ❑ Print an alphanumeric printout of the contest, candidates, position numbers, and vote totals when the polls are open to assure that all vote totals are at zero (0). At the close of polls, the voting machine must be able to print out in the same format the results of the election. These printouts should contain the voting machine serial number, the public counter total and the protective counter number. The poll worker must be able to request as many copies as necessary according to state law;
- ❑ Have the option of consolidating the vote totals for each candidate and question for an entire precinct onto one programmable memory device and the results of the precinct printed out at the precinct. This consolidating programmable memory device must be able to be brought into a central computer system and the results for that precinct read off of the programmable memory device so that a jurisdictional vote total report can be obtained;

- ❑ Have a mandatory pre-election testing of the ballot control logic and accuracy. The voting system also must have a post-election ballot control logic and accuracy test available after the election. These logic and accuracy test results must be stored into memory of the main processor and into the same programmable memory device that is used on election day for future reference. This should be stored by vote total summaries and by each individual ballot image randomly. The voting system must printout prior to these tests and a results printout after the test;
- ❑ Provide redundant storage of both the vote totals and the randomized individual ballot images. There must be polling of these multiple locations of totals and ballot images between voters to detect any errors or discrepancies. In the event of a data discrepancy, an appropriate error message must be displayed in order to either correct the data error or prohibit voting from continuing;
- ❑ Have a programmable memory device that plugs into the voting machine. This programmable memory device must contain the ballot control information, store the summary vote totals, maintenance log, operator log and the randomized ballot images which is each individual voter's choices. This programmable memory device must have the ability to be sealed in the voting machine prior to the election so that it is assured of not being tampered with without detection. This programmable memory device must be able to be removed after the polls are closed so that it may be brought to a central site where the vote totals can be read into a computer to obtain the jurisdiction totals;
- ❑ Be programmed with the ballot control information from the voting machine itself so that the results printout contains the candidate name next to the vote totals for the candidate;
- ❑ Be able to be programmed with the ballot control information by a separate computer which loads the information for that particular election into the programmable memory device. This same computer must be able to read the programmable memory device after the election to obtain the voting results and be able to accumulate the vote totals for the entire voting jurisdiction by precinct;
- ❑ Have a mandatory testing system to verify that the voting machine is in an operable condition within a reasonable period of time prior to an election. This testing must appear in the operator log of the system to verify that the tests were performed;
- ❑ Be able to test all major subsystems and assemblies in the software of the system;
- ❑ Have a mandatory verification of the ballot by the technician when setting up the voting machine for an election. This verification must check the ballot control information to see that the information on the ballot face is correct;
- ❑ Have an automatic means of voting the voting machine (voter simulation) in the warehouse to test the voting machine while the voting machine is only in the pre-election or post-election state;
- ❑ Maintain an operator log that begins with the resetting of the voting machine and continue throughout the complete election process. Next to each event should be printed the time and date;
- ❑ Allow voters from any voting precinct to vote at any location within the Parish;
- ❑ Allow units used during early voting to be de-programmed and re-programmed for use on election day, if necessary;

- ❑ Provide a means of electronically integrating absentee voting by mail results with voting system;

POWER SUPPLY:

- ❑ Have a self-contained, internal battery backup that is rechargeable by the main power supply when the voting machine is plugged into AC power. This battery must be commercially available. The battery supply must be capable of operating the voting machine without AC power for four (4) to twelve (12) hours;
- ❑ Have a main power system and battery charger that operate from a standard 115-volt, 60hz, single phase, alternating electrical current;
- ❑ Have a backup battery that powers all necessary components of the voting machine;
- ❑ Have backup battery power that in the event of a power outage in the precinct will be engaged with no disruption of operation or loss of data;
- ❑ Have a visible indicator that shows if the voting machine is receiving AC power. The voting machine must be able to test the battery and show the battery charge level. The voting machine must automatically shut itself down in the event the backup battery has only enough power to print out the results and go to an inactive state so to conserve enough power to close the polls at the end of the day;
- ❑ Remain operable in the event of abnormal line voltage conditions of power surges up to 132.25 volts rms over periods of up to two (2) seconds with a maximum of two (2) such surges per 60 second period;

SPECIAL FEATURES:

- ❑ Contain a gong or other sound creating device which will audibly indicate that a voter has left the machine after casting his vote;
- ❑ Provide visual and audible signals to the poll workers that the voting machine is in a voter active position and that the voter has cast their vote. The audible sound should be able to be heard from 20 feet. The visual display shall be well illuminated and easily readable;
- ❑ Have an adjustable volume control such that the bell, gong or noise making device signaling the casting of a vote is audible to the voter;
- ❑ Have all circuit boards conformal coated or provided with some other treatment which purpose is to significantly improve the reliability of circuit boards over a large period of time when used in an ambient air environment that is normal in the State of Louisiana (i.e. salt, dust, high humidity, rapid temperature changes);
- ❑ Must have components made of non-corrosive material or painted metal where required for strength;

EASE OF USE:

- ❑ Display clearly to the voter the mechanism by which his vote is cast;

- ❑ Have maximum weight to be handled by the poll worker while moving the voting machine or setting up the voting machine of not more than twenty-five (25) pounds;
- ❑ Have a display in full view of the voter that confirms the voter's choice;
- ❑ Be able to change his selections of candidates and questions on the ballot prior to casting his ballot. When deselecting the voting machines must verify to the voter on a display in full view of the voter that the de-selection was made;
- ❑ Allow poll workers to display the public and protective counters during an election;
- ❑ Be able to display such that poll workers can see any error messages associated with machine malfunction;
- ❑ Accommodate physically handicapped voters, particularly voters confined to wheel chairs, with little or no intervention by the poll worker;
- ❑ Permit voters to cast ballots as quickly as possible without any loss of degree of accuracy;
- ❑ Provide on-screen instructions to provide for voter awareness of the voting machine operation;
- ❑ Provide for an accurate and immediate transfer of data, if requested, to permit the dissemination of election results to the media and candidates in an expeditious manner;
- ❑ Present a ballot that is easy to read, follow legal requirements, be appealing to the voter's eye and include easy to follow instructions for use;
- ❑ Prompt voter when he is not using the device correctly;
- ❑ Make voter aware by clear means of ballot choice (i.e. a clear visual indicator that the voter has selected a particular candidate or proposition choice);
- ❑ Allow voter to review all ballot choices before casting the ballot;
- ❑ Provide sealed cases for transport to minimize damage to internal workings of the voting unit;
- ❑ Able to withstand frequent loading and unloading, stacking, assembling, disassembling, reassembling, and heavy use;
- ❑ Be stackable;
- ❑ Allow poll workers and Registrars' employees easy access to all activity taking place in the voting units, being able to monitor the movement of voters into and out of the voting booth;
- ❑ Have programmable memory device that is easy for poll workers and Registrars' employees to operate after the closing of the polls;
- ❑ Be "tamper-proof" while in a storage configuration either in the storage facility or the polling precinct;

REPORTING REQUIREMENTS

- ❑ Provide a cumulative, canvass and precinct report of absentee voting by mail, absentee voting by personal appearance and election day as one total;
- ❑ Provide a cumulative, canvass and precinct report of absentee voting by mail and early voting by personal appearance as one total;
- ❑ Provide a cumulative, canvass and precinct report of election day as one total;

- ❑ Provide for unofficial and official reports in any variety including absentee voting, election day and total vote;
- ❑ Provide the ability to custom design an election report to include the following information in total or in part;
 - 1) Name of election;
 - 2) Political subdivisions involved – separate reports should be available for each subdivision in the format enumerated above;
 - 3) Date of election;
 - 4) Type of report;
 - 5) Total number of registered voters in each political subdivision and total number of registered voters in each variable race;
 - 6) Total number of registered voters in each voting precinct, including a sub-listing when the precinct is split;
 - 7) Formatting of election results by capturing election data embedded in the database and producing specialized reports, i.e. a report of Presidential vote by legislative district or commissioner precinct;
- ❑ Provide, for election night reporting, a listing of precincts reporting and a listing of precincts not reporting;
- ❑ Provide for the operator of the reporting system to change the appearance of the report by reformatting the data;
- ❑ Provide for the removal of an already counted precinct and a re-counting of that same precinct in the event of errors in transmission;
- ❑ Provide individualized sample ballot information for storage on the Parish Clerk of Court's website and for reproduction and distribution;
- ❑ Provide for the automatic transmission of election results through electronic data, while adhering to the transmission rules set out in the Louisiana Election Code;
- ❑ Provide for the storage of election results in any version of software required, including, but not limited to, Access, Excel, Adobe, and ASCII;
- ❑ Provide for election results to be produced in such a manner as to allow for easy copying for paper distribution upon request; and
- ❑ Provide for the combining of election day, absentee in person, and mail-in absentee vote totals into the new counting system to achieve total votes.

I hereby adopt the above requirements as the voting machine certification standards for the State of Louisiana and Department of Elections and Registration, pursuant to La. R.S. 18:1351 and 1353.

Signed this 18th day of August, 2001.

S/ Suzanne Haik Terrell

SUZANNE HAIK TERRELL, COMMISSIONER OF ELECTIONS

consulting

Gartner



Brewer Voting Action Plan

Arizona Secretary of State's Office, Election Services Division