UNIVERSITY of ALASKA ANCHORAGE

State of Alaska Election Security Project

Phase 2 Report

Prepared for Lieutenant Governor Sean Parnell
and the State of Alaska Division of Elections

May 16, 2008
Final Report

This page left intentionally blank

Executive Summary
Alaska Election Security Report, Phase 2

See the back page for a list of contributors

University of Alaska Anchorage April 2008

Alaska's election system is among the most secure in the country, and it has a number of safeguards other states are now adopting. But the technology Alaska uses to record and count votes could be improved—and the state's huge size, limited road system, and scattered communities also create special challenges for insuring the integrity of the vote.

In this second phase of an ongoing study of Alaska's election security, we recommend ways of strengthening the system—not only the technology but also the election procedures. The lieutenant governor and the Division of Elections asked the University of Alaska Anchorage to do this evaluation, which began in September 2007.

The Division of Elections itself first identified a number of possible security improvements, and we evaluated their feasibility and potential benefits. We also identified additional improvements.

The table shows our main recommendations, dividing them into changes the state could make before the 2008 primary and general elections and changes that would take longer to put into effect.

The biggest recommendation is that the state upgrade all its technology to a new system recently developed by Premier Election Solutions, which manufactures the voting machines and related technology Alaska and other states use.

That new system is important. It corrects a number of vulnerabilities in the current system, identified in Phase 1 of this study. But as of April 2008, it had not yet been certified to standards required by the federal Election Assistance Commission. Alaska can't use the new system until it is certified—and when it is certified, it will take a lot of time, money, and people to do the upgrade. It will have to be installed on hundreds of optical-scanning machines, touch-screen devices, election-management servers, and other equipment scattered throughout Alaska. Taking on such a big, expensive job would not be practical, even if the new system were certified in the next few months. At this point, the Division of Elections is already doing many tasks required before the primary election in August and the presidential election in November. Also, because the state shares voting equipment with local governments, the upgrade will have to be coordinated with them as well.

But between now and the election, the state can improve security, with the changes recommended below. After the election, it can upgrade to the new system and develop a method for continuously monitoring changes in technology. We also recommend improving the way voting equipment is transported, tracked, and stored—as well as increasing the number of poll workers and providing them with more training in election security.

Recommendations for Improving Alaska's Election Security

Change By 2008 Election	Why?	Change After Election	Why?
✔ *Verify the accuracy of voting technology before and after the election, by comparing code in voting machines with correct, registered code*	This series of changes in technology and election procedures will make the existing technology more secure; improve security procedures among election officials and poll workers; and help increase Alaskans' confidence in the integrity of state elections. These measures can all be taken in the short-term, before the August primary and the November 2008 election.	✔ *Upgrade voting machines and other technology to new, improved platform*	Installing the new platform is the single-most important change the state can make, because it will reduce or eliminate risks of vote-tampering identified in the current system. But the platform must first be certified to the Election Assistance Commission's 2002 Voting System Standards, and after that will require an estimated 1,000 man-hours to install on election equipment statewide. Even if it were certified soon, it is not practical now to install the upgrade before the 2008 elections, given the time, expenses, and logistics involved. The other post-election recommendations are either longer-term enhancements of measures recommended for 2008, or additional security measures that there isn't time enough to implement before the 2008 elections.
✔ *Install new software that allows election officials to create a more-secure password authentication system for touch-screen machines*		✔ *Establish long-term security goals and a method for measuring progress*	
✔ *Change passwords on all voting technology throughout the system*		✔ *Improve testing processes to insure all voting technology is functioning properly and recording votes accurately*	
✔ *Use tamper-evident seals on shipping cases and envelopes*		✔ *Develop and implement a standard plan for tracking and changing passwords*	
✔ *Add election-security material to poll workers' training manual*		✔ *Improve system for tracking the number and location of voting machines, through bar-codes or other inventory-control measures*	
✔ *Increase vigilance about security procedures in absentee polling locations*		✔ *Strengthen storage facilities for voting machines and other system components with dead-bolt locks, alarms, ceiling grids, self-locking doors, and other features to prevent forced entry*	
✔ *Purchase state-owned voting machines for use in North Slope Borough, rather than borrowing borough-owned machines*		✔ *Buy more-secure shipping containers for optical-scanners*	
		✔ *Recruit and train more poll workers*	
		✔ *Consider partnerships with other institutions to do ongoing evaluation and implementation of changes in election-security technology*	

What is the Current System?

This is a particularly appropriate time for this study, not only because election-security has become a prominent issue nationwide, but also because this year marks the tenth anniversary of Alaska's use of electronic voting technology.

Unlike other election-security studies, our study is examining not only voting technology but also policies and procedures that add to the security of the system.

Much of our work in the first phase of the study was assessing the existing election system. To provide background for our recommended improvements, here we first briefly summarize the existing system. The figures on this page and the facing page show how the current system is organized and how it works.

The lieutenant governor heads the election system, and the Division of Elections manages federal and state elections statewide. The state is divided into four election regions, which in turn have 439 precincts. Election regulations, procedures, training, and technology are the same throughout the state.

There are multiple steps in the voting process, from the time Alaskans go to the polls until the director of elections certifies the results (as the figure on the facing page details). The process includes a number of security features that make it among the safest in the country:

- A centralized voting system, with standard procedures and identical hardware and software throughout Alaska. This centralization minimizes opportunities for tampering and allows flaws identified in any part of the system to be corrected statewide.
- Paper back-ups for all votes. Although optical scanners do scan and count ballots in 290 of Alaska's 439 precincts, almost all Alaska voters mark paper ballots that serve as back-ups to electronic tallies. There are touch-screen machines in all precincts. Only about 1% of voters use those machines, which also have internal paper reels as back-ups.
- Independent verification and cross-checking of paper ballots and preliminary electronic results.
- Audit of machine-counts of votes by hand-counts in a random sample of precincts.
- Observers invited to watch both voting and vote-counting procedures.

What Makes a System Secure?

Alaska's system has many strengths, but there is room for improvement. Alaska and other states use electronic systems to count and record votes. That technology has a number of advantages—it makes counting votes much faster, for example. Federal law also requires all polling places to have touch-screen devices for voters who can't mark paper ballots.

But election-security studies in other states have shown that the same voting technology voting used in Alaska could be vulnerable to tampering. Alaska also has security issues most other states don't face. It is huge—375 million acres—and the road system covers only about 10% of the land area. More than a hundred small communities can be reached only by water or air. Storms and intense cold frequently disrupt travel and shipments to remote communities.

Alaska's Election System

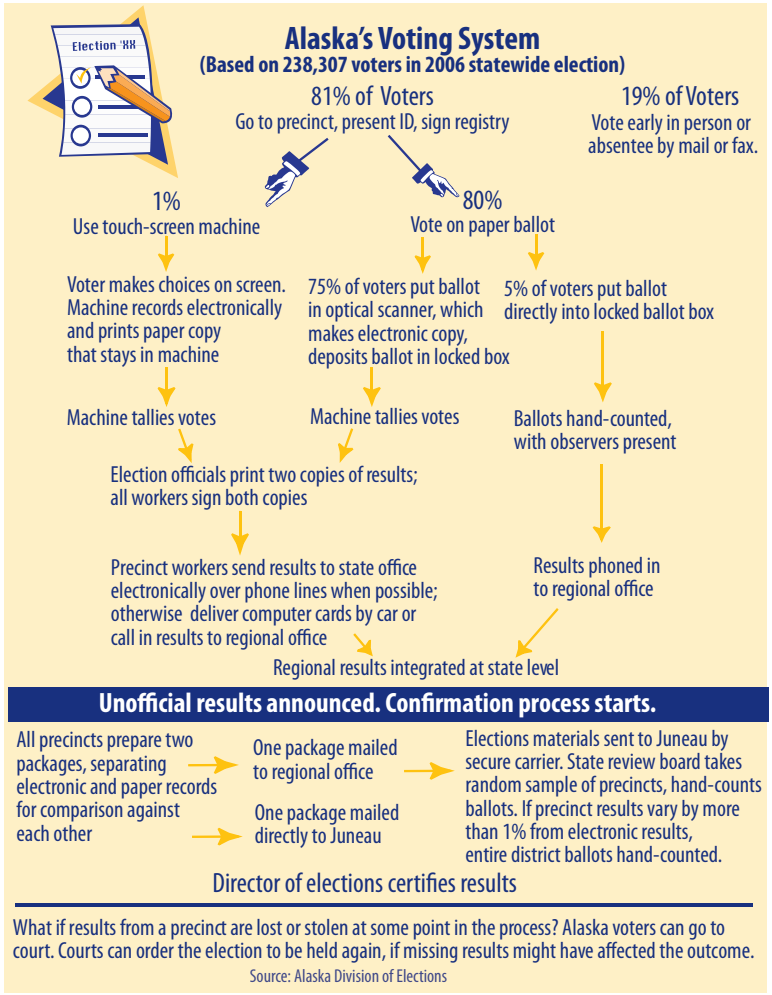
Lieutenant Governor	• Supervises Division of Elections • Appoints director of elections
Alaska Division of Elections	• Director of elections hires election supervisors for each region
Four Regions (Based on 40 House Districts)	
Regional Offices (Juneau, Anchorage, Fairbanks, Nome)	• Regional election supervisors hire bi-partisan election boards and supervisors for each precinct
439 Precincts (Large communities have multiple precincts)	• Precinct election chair-person hires bi-partisan election officials • Political parties, independent candidates, and groups sponsoring or opposing ballot initiatives may appoint observers to witness voting and vote-counting procedures

Source: Alaska Division of Elections

So sending ballots and election equipment to and from communities around the state, as well as storing equipment in small communities with limited facilities, is very expensive and poses many logistical challenges.

To evaluate how Alaska could improve security, we first thought about the elements that make a system secure, and grouped them into three categories: defense in depth, fortification of systems, and confidence in outcomes.

- *Defense in depth:* A secure system should have multiple layers of protection, so that if one fails others are still in place. This layered approach can discourage hackers, because they would have to take several undetected steps to penetrate the system's security. Also, layers can provide early warning of attacks in time for election officials to take action. Equipment, people, and procedures together provide defense in depth.
- *Fortification of systems:* This means making electronic systems as secure as possible and using the latest certified updates, which may correct vulnerabilities in earlier systems. Alaska uses optical scanners that tally votes cast on paper ballots; touch-screen machines with internal paper reels that record the votes cast; and servers that integrate and tally the electronic and hand-count results. All these system should be equipped with the latest updates to minimize the potential for votes to be miscounted or tampered with, and they should be protected so unauthorized users can't interfere with their operation before, during, or after elections. The systems must also be certified to federal standards and verified by independent testing centers.
- *Confidence in outcomes:* Systems and results have to be verifiable and shown to be reliable—to increase confidence of both voters and election officials in the system. The methods used to select a sample of results for hand-counting must also provide a high level of confidence. The election process must be open, so anyone can observe what is happening—and those who verify results must be objective and bipartisan.



Alaska's centralized processes and procedures at the state level make it easier to implement consistent security practices. Few states have such centralized systems, with standard practices and voting equipment statewide. Most states have decentralized systems—that is, systems in which counties, cities, or townships can set their own election procedures.

Also, Alaska's system provides a verifiable paper record of all the votes cast. Almost all voters mark paper ballots that are scanned and counted by an optical-scanner. About one percent of voters use touch-screen machines, with no paper ballots, but there is voter verifiable paper record .

The Pew Center for the States recently examined how many states have verifiable paper back-ups for votes. Keep in mind that most states have decentralized election systems—meaning individual counties or other local jurisdictions can choose their own methods—so the map illustrates the general rather than the exact situation in all states.

As the map shows, in 35 states all or most votes are backed up by paper records. In some of those states, voters mark paper ballots, which are then scanned and counted by optical scanners; in other states, voters mostly use touch-screen machines with internal paper reels.

But as of early 2008, 14 states primarily used touch-screen machines without paper reels. The Pew Center reports that two of those states—New Jersey and Maryland—have plans to implement paper-based systems. The remaining state, New York, still uses the lever-voting system, but almost all counties plan to begin using paper-based systems in 2009.

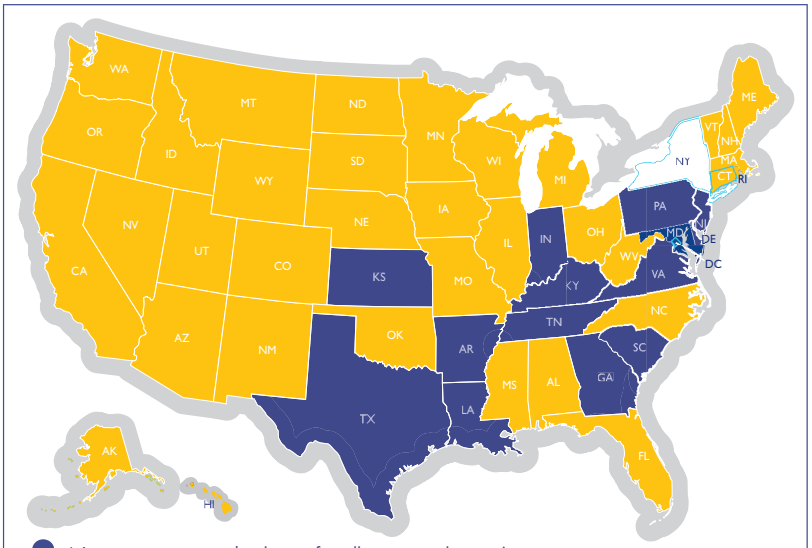
So overall the movement among states is toward systems with paper records—like the system already in place in Alaska.

How Did We Identify Security Issues?

- We studied the approaches taken in other states, to determine practices that could be helpful in Alaska.
- We evaluated the improvements the manufacturer of voting equipment has taken to correct security issues identified in other election-security studies and summarized in our Phase I report.
- We did a detailed, hands-on evaluation of storage, transportation, and packaging of election equipment and materials.
- We identified issues unique to Alaska, given our geographic diversity and transportation logistics.

We found that Alaska is well-positioned, compared with many other states. Alaska has in fact put into effect safeguards and processes that other states are now adopting to deal with election-security issues. But we also want to emphasize that every state faces different security and procedural challenges. There is no single solution right for every state.

We did find, however, that two aspects of Alaska's system help its election security, relative to that in other states: its centralization, and its paper ballot back-ups for virtually all votes.



14 states, no paper-back-ups for all or most electronic votes

35 states, some form of paper back-ups for all or most votes

1 state, lever-voting system

Notes: Many states use more than one voting technology. Not all states that have some paper back-up have complete paper back-up. New Jersey plans to have paper back-ups before the 2008 election; New York plans to adopt a paper-based system in 2009; Maryland law requires paper back-up by 2010.

Source: Based on Pew Center for the States, 2008

What Do We Recommend?

The table on the front page summarizes our main recommendations, some of which the Division of Elections could put into effect before the August primary and the November general election, and some of which it can't. Here we explain more about some of the most important recommendations, which are discussed in detail in the full report.

- ***Upgrade to the new, more secure platform after the election.*** We can't over-emphasize the importance of this upgrade. Alaska, California, Florida, and other states use the same or similar voting technology. Election-security studies in several states found that the existing technology was potentially vulnerable to vote-tampering in a number of ways. The new platform, (Premier Election Systems Assure 1.2), which the manufacturer developed in response to those studies, is still being tested to insure that it meets standards set by the federal Election Assistance Commission. We had hoped the system could be installed on Alaska's voting equipment by the 2008 election, but we now believe that's not feasible. Alaska is now in the run-up to the August primary and the November election. The Division of Elections is programming its equipment for those elections and doing other work that has to meet specific pre-election deadlines. Also, because the state shares voting equipment with local governments, the upgrade will have to be coordinated with them as well. To add in a huge, expensive job requiring complicated logistics at this point is not feasible. But we recommend that it be done as soon as possible after the election.

- ***Establish security goals and a method for regularly measuring progress toward those goals.*** The Division of Elections is well aware of security issues, and has taken a number of steps to improve security. But it currently has no long-range security goals nor a plan for measuring progress. We believe it's very important for the division to develop such goals and systematically meet them.

- ***Consider forming a partnership with some other organization that could continuously monitor and evaluate*** any new election-security vulnerabilities and ways to improve security. This would allow the Division of Elections to quickly make any necessary changes or improvements, before problems developed. Some states are already doing this. The Division of Elections itself does not have adequate staff to do such monitoring.

- ***Install new software that allows election officials to create a more-secure password authentication system for touch-screen machines***. Election officials are in fact already installing this new software, as they do programming for the upcoming election. This new software, called Key Card Tool, allows them for the first time to create their own authentication password and encryption keys for the state's 439 touch-screen machines. This is a substantial improvement in security. Previously, the default password and keys were in the public domain. They were programmed into all the touch-screen machines and couldn't be changed. Now, the password and keys can be changed regularly, and over time election regions could have their own individual passwords and keys.

- ***Verify the accuracy of voting technology.*** Before and after the November election, election officials should test all voting machines by comparing code in the machines with correct, registered code. In the longer-term, the state should develop standard testing processes to insure all voting technology is functioning properly and recording votes accurately.

- ***Change system passwords***. Before the election, the state should change all passwords currently used in election-system technology. After the election, the state should develop a plan for routinely tracking and changing passwords.

- ***Use tamper-evident seals on envelopes and shipping containers.*** This precaution can be taken before the upcoming election. Critics argue that attackers could in fact open such seals without leaving any evidence of tampering. But we believe that especially in Alaska—where ballots and equipment can travel long distances under difficult conditions—tamper-evident seals do help improve security.

- ***Recruit more poll workers and improve their election-security training.*** Before the election, the Division of Elections should add a section on election-security to the existing training manual, which doesn't currently discuss security. In the longer term, the state needs to recruit more poll workers—which in itself would help improve security in polling places—and to provide better training (possibly online) in election-security procedures.

- ***Improve the way voting machines are transported, tracked, and stored.*** Most of these recommended improvements can't be made until after the November election. They include buying better shipping containers for optical-scan machines, which have to be shipped to many small communities from larger regional centers before and elections and returned afterward. The state also needs a better system for tracking the number and location of voting machines, through bar-codes or other methods of inventory-control. Also, the physical security of machines in storage needs improvement. The state should consider reinforced doors, dead-bolt locks, ceiling grids, alarms, and other measures as appropriate.

Conclusions

We have made a number of recommendations for improving the security of Alaska's election system, but we want to keep those recommendations in context: Alaska's election system is in good shape. Other states are now adopting measures we've had in place for years. Personnel of the Division of Elections understand the system and have a good idea of what kinds of measures could help make it more secure.

But there's always room for improvement. Aside from the specific recommendations we've listed, Alaska needs to build a foundation for the future—to make sure Alaska's election system stays among the best in the country. The current election technology is aging, and the state will face new choices when it has to upgrade that technology. It needs to start systematically assessing its future needs and new technologies now.

This publication summarizes Phase 2 of the *Alaska Election Security Report,* prepared for Lieutenant Governor Sean Parnell and the Alaska Division of Elections. Contributors are LuAnn Piccard, Mark Ayers, David B. Hoffman, Stephanie Martin, and Kenrick Mock.

Table of Contents

List of Appendices

Glossary

Acronym/Phrase	Definition
AccuVote-OS or AV-OS	Premier Election Solutions optical scanning vote tabulation machine
AccuVote-TSX or AV-TSX	Premier Election Solutions touch screen voting machine
ADA	American with Disabilities Act
Chain of Custody	People, processes and locations of equipment and that have authorized custody of election material
DOE	Alaska State Division of Elections
DRE	Direct Recording Equipment (e.g. touch screen voting machine)
EAC	Election Assistance Commission
FEC	Federal Election Commission
ITA	Independent Test Authority
HAVA	Help America Vote Act
GEMS	Premier Election Solutions Global Election Management System
Memory Cards	Removable cards formatted with election information, used in optical scanning and touch screen voting machines to tally results
Premier	Premier Election Solutions formally Diebold
SAIC	Scientific Applications International Corporation
SAIT	Security and Assurance in Information Technology Lab (Florida State University)
TTBR	California Top-to-Bottom Review (commissioned summer 2007)
VSS	Voting System Standards
VVPT	Voter Verifiable Paper Trail
VVS	Voting System Standards 2002
VVSG	Voluntary Voting Systems Guidelines of 2005

Study Team

The analysis was conducted by a cross-organizational team from UAA and industry.

Principal Investigator
LuAnn Piccard, PMP, Instructor, Engineering, Science, and Project Management Department, School of Engineering, University of Alaska Anchorage

Cross-Organizational Team
Mark Ayers, P.E., Consultant, and Adjunct Faculty Member, University of Alaska Anchorage

Dr. David B. Hoffman, Adjunct Faculty and Consultant, University of Alaska Anchorage; retired Professor of Business Administration, University of Alaska Fairbanks.

Dr. Stephanie Martin, Assistant Professor, Institute of Social and Economic Research (ISER), University of Alaska Anchorage.

Dr. Kenrick Mock, Associate Professor of Computer Science, College of Arts and Sciences, University of Alaska Anchorage

Patricia Deroche, Research Associate, Institute of Social and Economic Research, University of Alaska Anchorage.

Mary Killorin, Research Associate, Institute of Social and Economic Research, University of Alaska Anchorage

Acknowledgements

The study team gratefully acknowledges help from many people.

Alaska Division of Elections
Division of Elections Director's Office

- Gail Fenumiai, State Director
- Shelly Growden, HAVA Election Systems Manager
- Jonathan O'Quinn, Election Program Manager

Region 1 Office (Juneau):

- Alyce Houston, Region 1 Election Supervisor

Region 2 Office (Anchorage, Mat-Su):

- Denali Elmore, Region 2 Election Supervisor
- Carol Thompson, Absentee and Petition Manager

Region 3 Office (Fairbanks):

- Shelly Growden, prior Region 3 Election Supervisor

Division 4 (Nome):

- Becka Baker, Region 4 Election Supervisor

Premier Election Solutions

- Kathy Rogers
- Don Vopalensky
- Ian Piper
- Dana LaTour

University of Alaska

- Fran Ulmer, Chancellor, University of Alaska Anchorage
- Diane McLean, Director Intellectual Property and Licensing

Interviewees from Alaska Cities and Boroughs

- Sherry Biggs, CMC, Borough Clerk, Kenai Peninsula Borough
- Johni Blankenship, CMC, Deputy Clerk, Kenai Peninsula Borough
- Laurie Sica, CMC, Municipal Clerk, City and Borough of Juneau
- Mona Lisa Drexler, CMC, Municipal Clerk, Fairbanks North Star Borough
- Julie Cozzi, CMC, Borough Clerk, Haines
- Harriett Edwards, CMC, Borough Clerk, Ketchikan Gateway Borough
- Colleen Pellett, CMC, Municipal Clerk, City and Borough of Sitka
- Cathy Bremner, Borough Clerk, City and Borough of Yakutat
- Tina Anderson, Borough Clerk, Aleutians East Borough
- Sheila Burke, Borough Clerk, North Slope Borough
- Tina Anderson, Borough Clerk, Aleutians East Borough
- Kate Conley, Borough Clerk, Lake and Peninsula Borough
- Carol L. Freas, City Clerk, City of Kenai
- Barbara Gruenstein, Municipal Clerk, Municipality of Anchorage
- Marjorie Harris, CMC, City Clerk, Municipality of Skagway
- Helena Hildreth, Borough Clerk, Northwest Arctic Borough

- Nova Javier, CMC, Borough Clerk, Kodiak Island Borough
- Lonnie McKechnie, CMC, Borough Clerk, Matanuska-Susitna Borough
- Gail Pieknik, Borough Clerk, Denali Borough

Interviewees outside Alaska

- Debra Bowen, Secretary of State and Lowell Finley, Deputy Secretary of State, California
- Stephen Weir, County Clerk, Contra Costa County, California
- Michael Barnes, Assistant Director, Kennesaw State University, Georgia
- Orville Brewster (Bud) Fitch II, Deputy Attorney General, State of New Hampshire

Introduction

This report details our work in Phase 2 of the Alaska Election Security study. In this phase, we developed recommendations for improving the security of Alaska's election system—not only the technology, but also the election policies and procedures. That's different from most election-security studies done in other states, which mainly assessed the security of election technology. It is electronic technology that has received the most attention in national debates about election security, but the policies and procedures—and the people who carry them out—are critical parts of any secure system.

In September 2007, Alaska's lieutenant governor, Sean Parnell, and the Alaska Division of Elections commissioned the University of Alaska Anchorage to evaluate Alaska's election systems and processes to identify security issues that could jeopardize election results. The study is in several phases and will be completed before the November 2008 presidential election. It also comes at a particularly appropriate time, since this year marks the tenth anniversary of Alaska's adoption of electronic voting technology.

The lieutenant governor—who oversees the election process—and the Division of Elections were concerned about election-security issues raised in studies done in several states. They wanted an evaluation of Alaska's election system, to identify potential security issues and measures to improve security. The Division of Elections itself first identified a number of possible security improvements, and we evaluated their feasibility and potential benefits. We also identified additional measures to enhance security.

We want to emphasize at the outset that Alaska's election system is among the most secure in the country. As we reported in Phase 1 of this study, Alaska's system includes a number of safeguards that other states are now adopting. But there is room for improvement in the technology Alaska and many other states use to count and record votes. Also, Alaska faces security issues most other states don't have. The state is huge—375 million acres—and the road system covers only about 10% of the land area. More than a hundred small, remote communities can be reached only by water or air. Storms and intense cold frequently disrupt travel and shipments to remote places. So sending ballots and election equipment to and from communities around the state, as well as storing equipment in small communities with limited facilities, is very expensive and poses many logistical challenges.

The Phase 1 report, completed in December 2007, included an overview of Alaska's voting system and discussed how our system compares with that in other states. It also summarized the findings from detailed election-security studies conducted by other states that use voting technology the same or similar to that used in Alaska. Those studies found that the current technology was potentially vulnerable to vote-tampering in a number of ways. The report concluded with a description of areas that required more detailed evaluation in Phase 2. Before we talk about our methods and findings, we first briefly discuss why election-security is an issue nationwide and describe Alaska's election system.

Why Study Election Security?

Almost all American voters now typically use some type of electronic voting equipment when they go to the polls—for instance, optical scanners that scan paper ballots and count votes, or touch-screen machines that may or may not provide any paper record of the vote. This technology has many advantages, including much faster vote-counting. Federal law also requires that all polling places have at least one machine for voters with disabilities that make it hard or impossible for them to mark paper ballots.

But many Americans are worried that these machines aren't secure—that they are vulnerable to tampering that could change the outcome of elections. The public must feel confident that every vote will be counted, and counted accurately. A number of states have examined how vulnerable voting equipment is to tampering—and found that in fact it is vulnerable in a number of ways. As we get closer to the 2008 national election, several other states and individual Americans have raised additional concerns. As a result of election-security studies and widespread publicity about security issues, some states are making changes—for example, insuring that there are paper records of votes cast electronically.

This Election Security Project has two important objectives: to help ensure the security of votes Alaskans cast and to enhance voters' confidence in the Alaska election system. That second objective is as important as the first. It's not enough to make the system more secure if Alaskans still have doubts about it. Election security should be real, both in the protections built into the system and in the minds of Alaskans—who rely on that system to count and report their votes accurately and at the same time to preserve the secrecy of the individual ballot.

It's not a simple task to build a system that provides security, accuracy, and privacy. Too much or too little focus in any single area can compromise the whole system. For example, some people have suggested that voters who use electronic voting machines could be given "receipts" that record their votes, as a demonstration of the accuracy of the system. But such receipts would not only violate the privacy of voters, they could also be used fraudulently in vote-buying schemes, in which voters would be paid for their votes after they demonstrated that they voted in a particular way.

What About Alaska?

Alaska's voting machines and other technology are manufactured by Premier Election Solutions, and are similar to equipment used in many states. The technology includes optical-scanners that scan and count votes cast on paper ballots; touch-screen machines with internal paper reels that record the votes cast; and computer servers that integrate and tally the votes. Almost all Alaska voters (99%) mark their choices on paper ballots; about 1% use touch-screen machines with internal paper reels.

Another critical part of the election system is the processes and procedures. We learned in Phase 1 that the election system includes a number of procedures that enhance security. The Phase 1 report includes a complete description of those security features, but below we summarize them briefly.

- *A single voting system, with standardized procedures and identical hardware and software, throughout the state*. This centralization of Alaska's system means that it is less complex, and it is simpler to evaluate and implement technology and procedures

statewide. Few other states have such centralized systems. For many reasons—including geography, population, history, and other factors—many states have more decentralized systems where counties, cities, or townships can make their own decisions about equipment, processes, and procedures. There is no single "right" system for all states, but Alaska's centralized approach has many benefits for election security.

- *Paper records of all votes casts*. As we noted above, almost all Alaska voters use paper ballots, and for the 1% who use touch-screen machines, there is an internal paper record. Many states have become increasingly aware of the importance of having paper back-ups. The map below, based on information from the Pew Center for the States, shows how many states have paper back-ups for votes as of early 2008. Keep in mind, however, that because most states have decentralized systems—that is, local jurisdictions can choose their own methods—the map illustrates the general rather than the exact situation in various states. In 35 states, all or almost all votes are back up by paper records. In some of those states, voters mark paper ballots, which are then scanned and counted by optical scanners. In other states, voters mostly use touch-screen machines with internal paper reels. But in early 2008, 14 states primarily used touch-screen machines without internal paper reels to provide back-ups. The Pew Center reports that two of those states—New Jersey and Maryland—have plans to implement paper-based systems. One state—New York—still uses the lever-voting system, but almost all counties plan to begin using systems that provide paper records in 2009. So overall the movement among states is toward systems with paper records—like the system Alaska already has in place.

- *Hand-counts of votes from a statistical sample of precincts across the state*. A state review board verifies the machine counts by hand-counting votes from a sample of precincts. If the hand-count results vary by more than 1% from the machine-counts in any particular precinct, votes from all precincts in the district will be hand-counted.

- *Bipartisan oversight of polling places*. Bipartisan committees oversee polling places, and political parties, independent candidates, and supporters or opponents of ballot initiatives can appoint observers to witness voting, vote counting, and vote audit procedures. Members of the public are also allowed to witness these activities.

- *Independent verification and cross-checking of paper ballots and preliminary electronic results*. Precincts separate ballots and electronic records and send them to both regional election offices and the Alaska Division of Elections for independent verification of results.

Approach to Phase 2

In Phase 1, we identified the elements that make for a secure election system, and grouped them into three categories: defense in depth, fortification of systems, and confidence in outcomes. We used those categories as a framework for assessing the level of risk presented by different security issues and for developing a set of high-priority recommendations. Some of those recommendations can be implemented during the 2008 election cycle and others will have to be done after the election. Here's how we define the parts of a secure system.

- Defense in depth. By that we mean a secure system should have multiple layers of protection, so that if one layer fails, others will remain in place. For one simple example of such depth, Alaska's electronic tallies of votes are backed up by paper ballots, measures are taken to keep the voting systems secure, and the electronic counts are verified through hand-counting a random sample of ballots. This example represents three layers of security, each of which would have to be breached in order to corrupt the election results. One of these elements might be subject to an attack or a mistake, but it is extremely likely that errors or problems would be caught by one of the other layers. Another example would be adding tamper-evident seals on the shipping packages, as well as on several parts on the outside and inside of the equipment. One exterior seal might be broken, possibly not intentionally but just while some equipment was being transported. However, if other internal seals remain in place after a systematic check of the equipment has been conducted, the equipment itself may still be secure. This is another example of a three-level defense in depth: external shipping container seals, external and internal equipment seals, and a systematic check of the equipment for evidence of tampering. We can think of defense in depth as a set of inter-related checks and balances that work together to enhance system security.

- Fortification of systems. Here we mean making electronic systems as secure as possible and using the latest updates, which often correct vulnerabilities found in earlier versions of the systems. This category also includes safeguards that ensure only authorized personnel have access to the system and that this access is properly controlled. Also, Alaska's unique conditions have security implications—for instance, voting machines are subject to temperature and transportation extremes not found in many other locations. And by law, systems used in Alaska must conform to the 2002 Voting System Standards (VSS). This equipment certification must come from a recognized Independent Test Authority (ITA).

- Confidence in outcomes. This means having systems and results that can be verified and shown to be reliable and that therefore earn the public's trust. Given the widespread distrust of electronic voting systems, this is critical. One way of building trust is being open about the system—letting voters and interested parties observe and participate in the process. Another way is keeping people informed about problems that have been identified and solutions being implemented to correct them. The intent is to correct as many issues as possible. However, in some cases after an evaluation of the costs and benefits, a decision might be made

not to correct certain issues that have a low potential for occurrence and that wouldn't have much effect if they did occur.

Multi-Phase Project

We're carrying out this project in several phases, each timed to coordinate with critical milestones in the 2008 election cycle. In Phase 1, we studied the work conducted by other states, determined its applicability to Alaska, and recommended areas for more detailed evaluation. In Phase 2, we conducted this more detailed analysis and are making detailed recommendations for consideration by the Division of Elections, for implementation in this election cycle and later. Phase 3, as determined by the Division of Elections, will provide assistance in implementing key recommendations, and Phase 4 could be a real-time system and procedural audit to verify the results of the recommendations that have been implemented. A potential Phase 5 might involve future work with the Division of Elections in the off-election cycle.

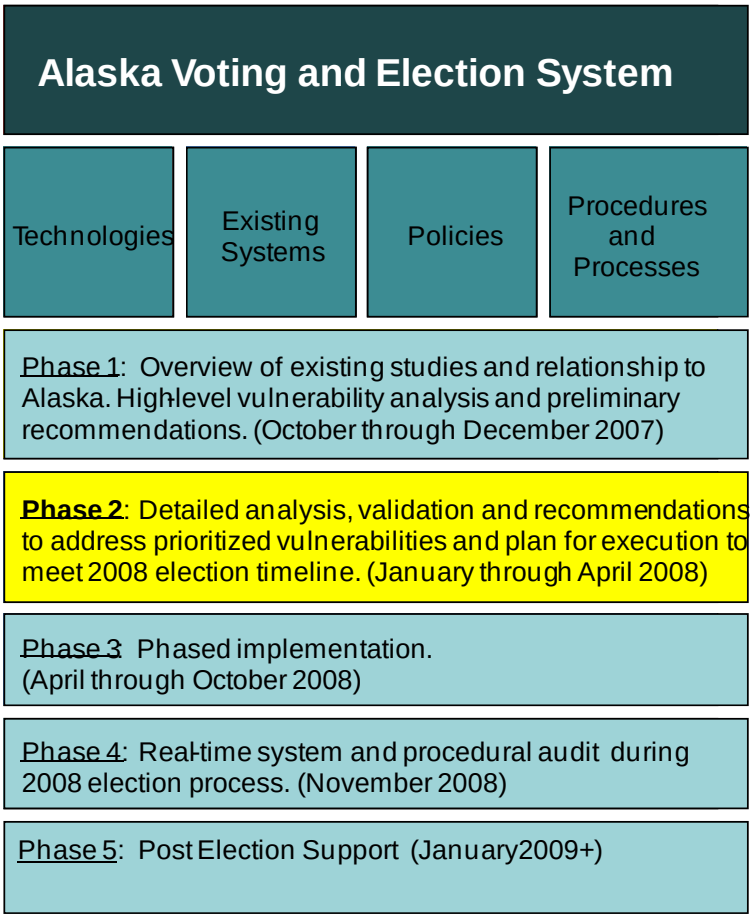


Figure 2.0 Multi-Phase Project

Scope of Work for Phase 2

The scope of work listed below summarizes the items that were selected for detailed study, grouped into the categories of defense in depth, fortification of systems, and confidence in outcomes.

Purpose: Detailed analysis of equipment and procedures and prioritized recommendations to improve Alaska election security.

1. Defense in Depth

1.1. Evaluate the cost and process to upgrade existing Premier system software and firmware if newer versions are available and certified in time to prepare for the 2008 election cycle. This analysis will be completed regardless of whether the software revisions are certified in time to implement the upgrades during the 2008 election cycle. Evaluate existing service and maintenance agreements with Premier.

1.2. Evaluate the upgraded Premier system software and firmware changes that have been submitted to the EAC for VSS 2002 Certification against potential and known security vulnerabilities identified in the Phase 1 report and as they relate to the security enhancements proposed by the Division of Elections. Summarize the original issue or concern and how the new version of Premier software and firmware may address (or may not address) the issues. (See attached document provided by Division of Elections for detailed list of items.)

1.3. Evaluate the existing Premier system software and firmware currently in use in Alaska. Determine if the security enhancements proposed by the Division of Elections can be implemented if current versions of tabulation software and firmware remain in use.

1.4. Provide recommendations to the Division of Elections on how existing procedures can be improved to address any identified security issues.

1.5. Evaluate password management options, recommend alternatives and propose appropriate processes and procedures.

1.6. Document inter-election chain-of-custody for voting equipment. With the knowledge that voting equipment is out of the DOE's custody during points in the election process, assess the risks of tampering, damage, and loss and provide recommendations to mitigate those risks.

1.7. With the knowledge that Alaska, for logistical purposes, stores touch screen and optical scan units off site between elections, determine best practices for storage and determine whether they would be feasible in Alaska communities. Recommend solutions that can meet security requirements and can also be practically implemented in the Alaska environment.

1.8. Identify trusted personnel within the Division of Elections and their points of access to equipment. Identify points of equipment access where only one person has access or authorization.

1.9. Determine points in election system where more redundancy in personnel, processes and /or joint review processes should be implemented.

1.10. Assess vulnerability of paper ballots to tampering. Contrast with risks in electronic system.

1.11. Summarize the security vulnerabilities of the equipment and procedures. To the extent possible, demonstrate the level to which proposed enhancements (equipment and procedures) mitigate security risks.

1.12. Develop security training procedures that can be included as an addendum to existing training documentation.

2. Fortification of Systems

2.1 Assess the integrity of the hardware and software of the electronic voting systems and their ability to accurately tabulate and report results.

2.2 Evaluate communication protocols and make recommendations regarding data transmittal to GEMS to avoid the introduction of viruses and longtime delays in election returns.

2.3. Evaluate the reliability and accuracy of the optical scanning and touch screen systems and their ability to function properly in Alaska weather and transportation/handling conditions. Study existing Premier reliability testing levels and equipment maintenance procedures to identify any concerns.

3. Confidence in Outcome

3.1 Evaluate processes and procedures DOE uses for functionality testing and logic and accuracy testing of systems and memory cards.

3.2 Identify methods DOE can use to increase voter confidence.

3.3 Establish metrics that the DOE can use to demonstrate continuous improvement of election security and predictability of results over time.

3.4 Provide a weekly review of emails from the public on security issues and summarize and publish general responses to them on Division of Elections website. Participate in other forums as requested by Division of Elections.

3.5 Provide a description of the absentee and questioned ballot process.

3.6 Research other random sampling methodologies that might provide additional confidence in election results. These recommendations would be proposed for future consideration and evaluation.

4. Evaluation and Implementation Plan

4.1 Synchronize Phase 2 work-plan with 2008 election process timeline to ensure that completion of critical evaluation deliverables and recommendations are phased with implementation deadlines as determined by the Division of Elections.

4.2 Develop project plan to implement prioritized recommendations (technology, systems and procedural) developed during Phase 2 work phased to meet 2008 election process timeline. If approved, this plan would be the basis of "Phase 3: Execution of Phased Deliverables."

Time Frame: Mid January 2008-end April 2008.
(Completion of deliverables will be phased throughout Phase 2 in accordance with section 4.1).

Cost (Est.): $250,000

Exclusions:

1. Detailed hands-on testing of the equipment in operation.
2. Destructive testing of equipment.
3. Payment for equipment, hardware, software firmware, tools, personnel, packaging, etc. required to upgrade election systems and procedures.
4. Usability analysis of touch screen systems (e.g. ease of use, language, user interface, set-up/tear-down, etc.)
5. Inventory analysis of existing equipment.
6. Documentation review and analysis.
7. Analysis of voter registration process.

Summary of Recommendations

We conducted analyses for each item on the scope of work listed above. Here we summarize the evaluation we conducted for each item of the scope of work and the relevant recommendations. More detailed information is included in the report appendixes, with the appropriate appendix cited in the summary.

Section	Scope of Work Item	Current Election Cycle Recommendation	Future Election Cycle Recommendation	Appendix Reference
		1.0 Defense in Depth		
1.1	Assure 1.2 Upgrade Cost Analysis	Maintain current revision of AccuVote software, perform cost benefit analysis to determine best resource utilization approach.	Upgrade to Assure 1.2 when certified	Appendix A - Assure 1.2 Upgrade Labor Estimate
1.2	Assure 1.2 Functionality Upgrade Analysis	Maintain current revision of AccuVote software.	Upgrade to Assure 1.2 when certified	Appendix B - Assure 1.2 Upgrade Analysis Appendix C - Assure 1.2 Upgrade Resolution Matrix
1.3	Division of Elections Security Enhancements and Features Analysis	Implement selected recommendations from Appendix D - Division of Elections Enhancement Analysis. 2.1-2.5, 2.8, 2.10, 2.13, 2.16, 2.18, 2.19, 2.23, 2.29	Implement remaining recommendations included in Appendix D.	Appendix D - Division of Elections Enhancement Analysis
1.4	Implement procedures to minimize technology risks not addressed by existing or upgraded systems	Implement procedures described in other sections. Important to maintain many of the processes already in place.	Monitor research on election processes and implement changes, as appropriate.	
1.5	Password Management	Change passwords on all affected hardware as outlined in password management plan (Appendix E).	Develop password management procedures to implement password changes and tracking for future election cycles to ensure password policies are followed consistently.	Appendix E - Physical Password Management Recommendations
1.6	Chain of Custody	Begin to use tamper evident seals on AV-OS and AV-TSX machines.	Further implementation of tamper evident seals. Implement EPROM bar code identification and inventory management.	Appendix G

Section	Scope of Work Item	Current Election Cycle Recommendation	Future Election Cycle Recommendation	Appendix Reference
		1.0 Defense in Depth (cont.)		
1.7	Best practices for equipment storage between elections	Follow Chain of Custody recommendations. Purchase Division of Elections owned equipment for North Slope Borough. Safes are recommended for use in Division of Elections offices to store keys and passwords.	Improve physical storage security such as room security, access alarm, etc.	
1.8	Trusted Personnel and single points of access	None	Require background checks on new employees with access to election equipment and confidential information	
1.9	Redundancy	Two person inspection and sign off on tamper evident seals.	Add two-person sign-off to manual entry of election results and tamper seal inspections.	
1.10	Paper Ballot tampering vulnerability	None	None	
1.11	Master Vulnerability Matrix	N/A	N/A	Appendix R - Master Matrix Recommendations, Risk and Value Assessment Appendix S - 2008 Election Cycle Impact Matrix Appendix T - Future Election Cycle Impact Matrix
1.12	Security Training	Develop materials to train poll worker in election security.	Monitor new procedures and expand training as appropriate.	Appendix H

Section	Scope of Work Item	Current Election Cycle Recommendation	Future Election Cycle Recommendation	Appendix Reference
2.0 Fortification of Systems				
2.1	Assess the integrity of the hardware and software of the electronic voting systems and their ability to accurately tabulate and report results.	Implement Key Card Tool application. Implement GEMS Air Gap Server model system. Implement dedicated AV-OS machine for programming AV-OS memory cards.	None	Appendix O - Security Key Card Enhancement Options Appendix P - Security Key Card System Description Appendix M - AccuVote Functional Test Guidelines
2.2	Preliminary Results Data Collection Assessment	None	None	Appendix J - AccuVote Communications System Description Appendix K - AccuVote Network Topology
2.3	Evaluate the reliability and accuracy of the optical scanning and touch screen systems in Alaska weather and transportation/handling conditions.	None	Implement new shipping containers for optical scanning systems (PelicanTM. Products 1600 series or similar)	Appendix L - AccuVote Reliability Assessment Appendix I - AV-OS Shipping Container Example

Section	Scope of Work Item	Current Election Cycle Recommendation	Future Election Cycle Recommendation	Appendix Reference
3.0 Confidence in Outcomes				
3.1	Procedures for functionality, logic and accuracy testing for systems and memory cards.	Implement increased test scope for functional, logic and accuracy testing.	Implement test results documentation and storage policies.	Appendix M - AccuVote Functional Test Guidelines Appendix N - AccuVote Logic and Accuracy Test Guidelines
3.2	Methods to improve voter confidence	Increase voter use of AV-TSX machines to improve voter anonymity.	Monitor research on election processes and implement changes, as appropriate.	
3.3	Metrics and continuous improvement	Implement a multi-year, multi-phase approach to improving election procedures and equipment.	Multi-year, multi-phase approach	Appendix F - Chain of Custody Map
3.4	Weekly email summary	Provide on-going summary	Provide on-going summary	
3.5	Absentee and questioned ballot process	Implement 2008 election cycle security improvements.	Same as current election recommendations.	Appendix Q - Summary of Absentee Voting
3.6	Random sampling methodologies	None. Current research is not conclusive enough to recommend a change to the Division of Elections methodology.	Implement new sampling procedure as appropriate and approved by statute.	

Part 1 Defense in Depth

Section 1.1 – Premier Election Solutions Assure 1.2 Software Upgrade Cost Analysis

Description:

Evaluate the cost and process to upgrade existing Premier Election Solutions (Premier) (formerly Diebold) system software and firmware if newer versions are available and certified in time to prepare for 2008 election cycle. This analysis will be completed independently of whether the software revisions are certified in time to implement the upgrades during the 2008 election cycle. Evaluate existing service and maintenance agreements with Premier.

Summary of Analysis:

The cost to upgrade from the existing AccuVote software and firmware revisions consists of contributions from two different upgrade components.

The first component is the cost to purchase the software and firmware components from Premier. The Division of Elections has a current maintenance agreement with Premier which includes software and firmware upgrades at no additional cost.

Implementation of the Assure 1.2 upgrade requires software and firmware upgrades to be performed on all major AccuVote system components. The labor estimate table provided in Appendix A – Assure 1.2 Upgrade Labor Estimate provides a list of the tasks required to be completed for the Assure 1.2 upgrade as well as an estimate of 995 person-hours to implement a system-wide firmware/software upgrade AV-OS, and AV-TSX. Labor associated with each upgrade task is provided as estimated hours. Actual hours were not measured for the purposes of this report. The comprehensive nature of the Assure 1.2 upgrade requires that a complete acceptance test be performed following the upgrade to ensure system functionality and reliability.

Recommendation:

2008 Election Cycle

We recommend that the Division of Elections do a cost benefit analysis to determine whether performing the upgrade using Division of Elections resources, external contractors or contracting with Premier is a more cost effective approach for implementing Assure 1.2.

Post Election

We recommend implementing the Assure 1.2 upgrade upon certification by the Election Assurance Commission (EAC) to the Voting Systems Standards (VSS) 2002 using the resources deemed most cost effective in the 2008 election cycle.

Section 1.2 – Premier Election Solutions Assure 1.2 Software Upgrade Enhancement Evaluation

Description:

Evaluate the upgraded Premier system software and firmware changes that have been submitted to the federal EAC for VSS 2002 certification against potential and known security vulnerabilities identified in the Phase 1 report and as they relate to the security enhancements proposed by the Division of Elections. Summarize the original issue or concern and how the new version of Premier software and firmware may address (or may not address) the issues.

Summary of Analysis:

Phase 1 of the State of Alaska Election Security Project (SOAESP) examined the current body of knowledge surrounding the Premier AccuVote voting system platform. This examination was focused on identifying areas of vulnerability within the AccuVote system currently in use by the Division of Elections. Phase 1 of the SOAESP reported that research conducted by the states of California (Calandrino, et al., 2007; Bishop, 2007), Florida (Gardner, et al., 2007) and others found vulnerabilities in the AccuVote platform currently in use by the Division of Elections as well as many other states. Premier responded to this research by producing revised versions of the software and firmware that operate on various components of the AccuVote system and address a number of the identified vulnerabilities.

An examination of the AccuVote software, firmware and hardware components used by the Division of Elections as well as an analysis of the vulnerabilities identified by the states of California, Florida and Alaska are provided in Appendix B - Assure 1.2 Upgrade Analysis. This appendix provides a summary description of each vulnerability or issue identified by California, Florida or Alaska. The status of each vulnerability is provided in tabular format in Appendix C – Assure 1.2 Upgrade Resolution Matrix.

A total of 38 individual vulnerabilities, issues or risks are identified and itemized for evaluation against the Assure 1.2 revision. These items are compared with the Assure 1.2 functionality to determine whether the vulnerability, issue or risk remains following the installation of the Assure 1.2 software or firmware. Installation of the Assure 1.2 revision reduces the number of vulnerabilities, issues and risks to 13.

By Alaska statute, the Assure 1.2 AccuVote revision must comply with VSS 2002 before it can be used in Alaska. Certification by an approved Independent Test Authority (ITA) is required to verify compliance to the VSS 2002 standard. At the time this document was written, the Assure 1.2 revision was under test by SysTest, an approved ITA, and certification had not yet been granted.

Recommendations:

The Assure 1.2 AccuVote revision includes significant improvements in overall system security performance. The system revision provides patches to public domain bugs, known vulnerabilities and system use issues.

2008 Election Cycle:

We do not recommend implementation of the Assure 1.2 upgrade during the 2008 election cycle. Since the Assure 1.2 revision has not yet been certified to the VSS 2002 standard, we cannot recommend that it be implemented prior to the 2008 election year primary and general elections. Furthermore, even if the software were to become certified prior to the elections there is insufficient time and resources to implement the revision before election programming must begin.

Post Election:

We recommend that the Assure 1.2 AccuVote revision be installed following the 2008 election cycle and once the appropriate VSS 2002 certification has been obtained.

Section 1.3 – State of Alaska Division of Elections Proposed Enhancement Evaluation

Description:

Evaluate the existing Premier system software and firmware currently in use in Alaska. Determine if the security enhancements proposed by the Division of Elections can be implemented if current versions of tabulation software remain in use.

Summary of Analysis:

The State of Alaska, Division of Elections has produced an internal document, *AccuVote Security Enhancements and Features* (2007). This document is a list of internally recommended security enhancements identified by the Division of Elections. A request was made of the project team to evaluate whether any or all of the proposed enhancements could be adopted within the structure of the currently operated AccuVote software, firmware and hardware platforms.

All of the recommended enhancements can be implemented on the current system with little to no impact on system performance. Implementation of the feature and enhancement list is limited by Division of Elections resource availability.

A detailed discussion of each feature or enhancement is provided in Appendix D – Division of Elections Enhancement Analysis. A cross-reference between the Division of Elections AccuVote Security Enhancements and Features and Appendix D – Division of Elections Enhancement Analysis is provided below.

Division of Elections Heading	Appendix D Section
GEMS Software and Computers	Sections 2.1 to 2.7
Memory Cards	Sections 2.8 to 2.16
Voting Equipment	Sections 2.17 to 2.25
Testing and Audits	Sections 2.26 to 2.28
Administrator Card	Section 2.29
City/Borough	Sections 2.30 to 2.31

Recommendations:

2008 Election Cycle:

We recommend that the Division of Elections implement selected recommendations from Appendix D - Division of Elections Enhancement Analysis. A subset of the recommendations in Appendix D (Sections 2.1-2.5, 2.8, 2.10, 2.13, 2.16, 2.17, 2.18, 2.19, 2.23, and 2.29) should be adopted during the 2008 election cycle. Highest priority should

be placed on hash validation, access control and password management, chain of custody assurance, and tamper evident security measures.

Post Election:

The balance of the enhancements not performed during the 2008 election cycle can be implemented between the 2008 and 2010 election cycles. This phased implementation approach will address the most critical issues first and provide an opportunity for the Division of Elections to balance multiple resource demands during this election year.

Section 1.4 – Procedural Security Enhancements

Description:

Provide recommendations for improving existing procedures to address security issues.

Recommendations:

2008 Election Cycle

Many of the Division of Elections' existing procedures work well and need to be maintained. Among these are post election precinct level reconciliation, post election audit, election officials as state employees (rather than political appointees), use of chain of custody, current ballot printing company, allowing/encouraging observers.

We recommend using tamper evident seals on election equipment (Section 1.7) and having poll workers inspect seals (Section 1.12), increasing poll worker awareness of tampering risks (Sections 1.6 and 1.12), implementing background checks for employees with access to sensitive information and voting equipment (Section 1.8), requiring two people to sign off on many procedures (Section 1.9), and ensuring that when voters use AV-TSX machines, at least five people vote on them (Section 3.2).

Post Election

Continue to monitor research on election processes and procedures. Make changes to Alaska's system as appropriate.

Section 1.5 – State of Alaska Division of Elections Password Management Options Evaluation

Description:

Evaluate password management options, recommend alternatives and propose appropriate processes and procedures.

Summary of Analysis:

The Division of Elections has a desire to improve its handling of passwords. The division manages several sets of security controls accessed by password to implement an election. These security controls consist of physical security, computer Built-in Operating System (BIOS) security, Windows operating system login security and Global Election Management System (GEMS) database security. These domains form a hierarchical password security system in which multiple levels of security penetration are required to gain access.

Physical security and access to servers and voting machines was found to be inconsistent across voting regions with some regions executing physical security in a more robust manner than other regions. The Division of Elections does not currently implement BIOS passwords on any of the GEMS servers in the AccuVote system. Additionally, although the Division of Elections currently uses a password management plan for its Windows login and GEMS database, room for improvement exists in the management of passwords for both of these security domains.

Appendix E – Physical Password Management Recommendations reviews the current Division of Elections password management policies and makes a series of recommendations regarding each of the security domains.

Recommendations:

2008 Election Cycle:

We recommend changing passwords on all hardware and software platforms as outlined in Appendix E – Physical Password Management Recommendations. Development of formal policies to accompany the password changes during the 2008 election cycle is not recommended due to resource constraints.

Post Election:

We recommend that the Division of Elections make improvements to the consistency and fortification of physical security access at equipment storage locations as well as implement structured password management policies for each password security domain within the AccuVote system. The structured password management policies should

include documentation guidelines and formal procedures associated with the implementation of the password management plan. A more detailed description of these recommendations is provided in Appendix E – Physical Password Management Recommendations.

Section 1.6 - Chain of Custody

Description:

Document the inter-election chain-of-custody for voting equipment. With the knowledge that voting equipment is out of the Division of Election's custody during points in the election process, assess the risks of tampering, damage, and loss and provide recommendations to mitigate those risks.

Summary of analysis:

We define "chain of custody" to mean traceability of secure storage and transportation of election equipment during all phases of an election cycle and in between election cycles. Election equipment includes: ballots, AccuVote optical scan (AV-OS), AccuVote Touch Screen (AV-TSX) machines, and memory cards. An overview of Alaska's chain of custody procedures for road connected communities and map of Alaska's chain of custody is included in Appendix F - Chain of Custody Map.

The chain of custody works well for sending election equipment among Alaska's larger and road connected communities. However, 41% of the state's precincts (179 out of 439) are off the road system and can only be reached by boat or airplane[1]. This represents about 17% of voters (77,000). As a result, chain of custody documentation is not feasible and secure storage space for election equipment may not be available. These conditions cause some of the election machines to be vulnerable to tampering during transit and storage. Additionally, many of the AV-TSX and AV-OS machines remain in communities between the primary election in August and general election in November[2]. Some municipalities and boroughs use the AV-OS machines in municipal elections in October. The AV-OS machines are outside of the state's chain of custody when used in municipal elections.

Prior to the primary election, OS machines are stored in regional centers, satellite offices or hubs. Several weeks before the primary election, the regional offices test AV-OS machines with their memory cards inserted. Memory cards are sealed inside the AV-OS machines and they are sent out to AccuVote coordinators in communities. Following elections, some machines are stored in communities, others are returned for storage in hubs or regions. Storage is less centralized between the primary and general election than prior to the primary. Memory cards are sent to AccuVote coordinators in communities where AV-OS machines have been stored. For the general election machines are again tested with their memory cards.

---

[1] Some have ice road access in the winter.

[2] Shipping AV-TSX machines back to regional hubs would double the shipping costs, and require more election staff. It is a logistical challenge to send AV-TSX machines (weighing 60 pounds), ballots (another 25 pounds), printers, voting booths, and ballot boxes by small air carrier to hundreds of remote communities.

Because of time and staffing constraints, AV-TSX memory cards are currently batch tested and inserted into machines on election day. The alternative would be to test each memory card in its AV-TSX machine, seal the card and ship the machines with cards inserted to precincts for primary elections, then ship all machines back to hubs or regional centers and repeat the process prior to the general elections. It is not feasible to ship all machines back to regional hubs and back out to precincts between elections. It would double the current transportation costs and more than double staff time. After the primary, Division of Elections staff members are busy preparing for the general election. To set up and test each AV-TSX machine with a memory card inside would take 30 minutes per machine. We estimate that it would take a minimum of 220 hours (about 5.5 weeks) to test machines one-by-one.

The North Slope Borough owns several AV-OS machines. In past state/federal elections the state borrowed AV-OS machines from the borough. The borough's machines are outside of the state's chain of custody and security domain. The state has addressed this problem by purchasing additional state-owned AV-OS machines to use in North Slope communities.

Recommendations:

2008 Election Cycle:

We recommend continuing to use the current system for shipping and testing AV-OS machines and their memory cards.

We recommend Division of Elections continues to ship AV-TSX memory cards separately from machines.

We recommend using tamper evident seals[3] on all AV-OS and AV-TSX machines. In collaboration with California counties, Premier developed best practices for use of tamper evident seals (Premier Election Solutions 2008). Appendix G - Premier Best Practices for Tamper Evident Seal Placement contains the Premier document. Although Premier recommends using two seals[4] on AV-OS machines and three seals on AV-TSX machines, we recommend that the Division of Elections adopt a phased approach to using tamper-evident seals. Because election equipment is shipped around the state and may be subjected to rough handling and harsh weather conditions, we recommend using one seal on each AV-OS and each AV-TSX machine in 2008. If there few false alarms and as seal inspection and reporting methods are fine tuned, we recommend increasing the number of seals per machine in future election cycles.

[3] We take into consideration the finding in California's top-to-bottom review that tamper evident seals are easy to remove and replace (Calandrino et al. 2007). We see implementing tamper-evident seals as a way to make attacks more difficult or riskier, but not necessarily impossible (Johnston 2006).
[4] Intab and Seton corporations manufacture seals used successfully in Premier tests

For AV-OS machines a serialized tamper evident security seal should cover either the front "seam" or the back "seam" and screw hole. Refer to Appendix G for Premier's illustrated documentation of security seal placement.

For AV-TSX machines; following Premier's recommendations, the seal should cover the "seam" and a screw hole on the back of the machine. (See pictures in Appendix G)

Memory cards: For locations where AV-TSX machines are stored between primary and general elections, we recommend mailing AV-TSX memory cards in tamper-evident envelopes or bankers bags.

In addition to using tamper-evident seals, we recommend providing poll workers with a check list and procedures for seal inspection and instructions for what to do if seals are broken. (See Appendix H - Security Training).

The regional office in Fairbanks currently uses a Microsoft Excel based inventory management system. We recommend using this system state-wide.

Post Election:

If using one tamper-evident seal on each machine is successful, we recommend expanding the use of tamper-evident seals in accordance with Premier's best practices. AV-OS machines: in addition to the seal over the front or back seam, the memory card slot should be sealed with serialized security seal. Refer to Appendix G for Premier's illustrated documentation of security seal placement.

AV-TSX machines: In addition to the seal over the seam, we recommend two additional tamper-evident seals on each AV-TSX unit. One of the seals should cover the memory card slot. The second seal should seal the privacy panels that cover the touch screen panel (See pictures in Appendix G). We also recommend using tamper-evident serialized seals on the metal shipping cases.

We recommend implementing a bar code system to keep track of equipment.

Section 1.7 - Storage of Election Equipment and Material

Description:

With the knowledge that Alaska, for logistical purposes, stores touch screen and optical scan unites off-site between elections, determine best practices for storage and determine whether they would be feasible in Alaska communities. Recommend solutions that can meet security requirements and can also be practically implemented in the Alaska environment.

Summary of analysis:

This refers to the physical storage of election equipment: ballots, memory cards, GEMS servers, and peripherals AV-OS and AV-TSX machines. We evaluate storage practices in Alaska given the logistical challenges and make recommendations that take them into account.

We visited and examined storage sites in Anchorage, Fairbanks, Juneau and Kenai and interviewed the regional director in Nome, Juneau and Fairbanks, all borough clerks, several municipal clerks. We also reviewed Premier/Diebold recommendations and other documents. Uniform practices for storing election machinery would be ideal, but differences in building construction and lease arrangements limit the ability of Division of Elections to implement a completely uniform storage practice. Storing AV-OS and AV-TSX machines in remote communities prior to and between elections complicates equipment storage.

Recommendations:

2008 Election Cycle

Regional and state storage areas should have a safe in the director's office for storage of keys and password codes.

We recognize that AV-TSX machines are big and take up a lot of storage space. If possible, in remote communities, equipment should be stored in a lockable closet within a municipal or tribal office. If such a facility is not available, machines should be stored in a facility that can be locked when the person responsible for the equipment is not present. Poll workers' training needs to emphasize the importance of secure storage.

For equipment in non-secure facilities, additional precautions including inspections, and functional tests should be conducted in advance of equipment use to ensure that any tampering or reliability issues can be proactively identified. (See Appendix H-Security Training.)

Post Election

- A monitored alarm system in all secure storage rooms
- Deadbolt locks on secure storage room doors
- Self-closing/locking doors
- Metal ceiling grids in locations where walls do not extend to the roof or upper floor structure.
- Keyless entry for secure storage rooms with automatic logging of entry and exit.
- Motion detection security cameras.
- For the state GEMS storage room in Juneau, we recommend relocating network switching equipment outside of the election equipment room.

The Division of Elections officials should consider the ease in securely storing and shipping equipment in their decisions about future equipment purchases.

Section 1.8 – Trusted Personnel and Single Points of Access

Description:

Identify trusted personnel within the Division of Elections and their points of access to the equipment. Identify points of equipment access where only one person has access or authorization.

Summary of analysis:

We interviewed Division of Elections staff to identify places in the system where a single person has access to software, machines, or election material. We found several instances of singular access. The GEMS programmer in Juneau, AccuVote coordinators, poll workers who store election equipment, and pilots and air carriers who transport machines all represent positions in the election system with singular access to election components. The GEMS database is a Jet database file (similar to Microsoft Access). Programming the election involves filling in fields in the interface. The GEMS program has built-in checks for errors and prompts the user to make changes. Several people besides the programmer review ballots before they are sent to the printer[5]. The Division of Elections has a small staff, some of whom have been at their jobs for almost 20 years. The system relies on a high degree of implied trust. Tampering with electronic results could be detected by the random audit conducted as part of every election.

Recommendations:

2008 Election Cycle:

We recommend continuing to use one person to enter elections information into GEMS. Having multiple people programming the elections database is problematic. Alaska's boroughs and municipalities that use GEMS and Kennesaw State University Election Center (which programs ballots for the state of Georgia) use one person to enter elections information into GEMS. The use of a single person is believed to result in fewer errors because one person is keeping track of changes to the system. The enhanced logic, accuracy, and integrity testing procedures increase the probability of detection of errors and issues with election programming prior to deployment for use.

Post Election:

For the positions of election programmer, regional director, and absentee director we recommend implementing a program of background checks for new hires, in accordance

[5] Boroughs and municipalities in Alaska use a similar system of proof-reading. Georgia loads a test ballot into the AV-TSX machine as part of the proof reading (however, over 99% of voters there use touch screen devices).

with state law and labor union agreements. We recommend that the Division of Elections recruit and train more AccuVote coordinators.

Section 1.9 – Redundancy

Description:

Determine points in election system where more redundancy in personnel, processes, and/or joint review processes should be implemented.

Summary of analysis:

Redundancy can not only protect the election system from tampering, it can also lower the chance of errors[6]. In election systems there is a trade-off between the proprietary nature of the election information and having staff redundancy to safeguard the system. Division of Elections has several people trained in GEMS programming, in addition, several borough level officials are also trained in GEMS programming. Elections could proceed if the primary programmer was unavailable due to extenuating circumstances. The state has seven people with access to GEMS: one with programming access, six with access at regional offices. The state requires two elections officials or poll workers present during logic and accuracy testing, and equipment packing for shipment to precincts. Joint review for some polling place tasks[7] is difficult in practice.

Recommendations:

2008 Election Cycle

Maintain current two-person sign-off on precinct level post-election practices of checking vote tallies and registration lists and reporting results.

Add second person or have cross-checking review for the following tasks:

- Verification of tamper-evident seal integrity.
- Verification of tamper-evident seal serial numbers.
- Manual entry of election results into GEMS.

Post Election:

Increase focus on poll worker recruitment.

---

[6] Despite all the attention devoted to potential tampering, researchers found that past problems with election results were due to human error or equipment problems, and not malicious intruders (Thompson 2008, Herrnson et al. 2008).

[7] Alaska's instructions for AV-TSX setting up recommend that one person read instructions, another set up the machine. Two people are also required to sign off on zero totals on AV-OS and AV-TSX tallies. People are also required to set up tables, post signs, assemble voting booths, and organize registration books and other voting materials. Sometimes all task need to be done within 30 minutes, by poll workers whose average age is 72. If a polling place is short staffed, its unlikely two people will be available for tasks.

Section 1.10 – Paper Ballot Tampering Vulnerability

Description:

Assess vulnerability of paper ballots to tampering. Contrast with risks in electronic system.

Summary of analysis:

Paper ballot tampering is easier to detect than electronic tampering because it takes more people, better organization, and a higher level of secrecy to tamper. (Norden, et al. 2007). Changing election results on a large scale by tampering with paper ballots scale requires widespread access.

Ballot stuffing is a one way to tamper with paper ballots. However, Norden et al. (2007) write that it would take several election insiders at each polling place to carry out a ballot stuffing attack. Insiders need to steal ballots, copy and mark them, insert extra ballots into the optical scanner or ballot box, and adjust voter registration books. Despite this potential attack scenario, the polling place post-election accounting process (comparing number of ballots cast with number of signatures in the registration book) would likely detect a ballot stuffing attack. A second process check at during the statewide audit of post-election results could also detect ballot stuffing.

Vote buying is another method of tampering with paper ballots. A vote buying scheme would involve hundreds of people and would require that hundreds of people keep quiet. People would also need to be able to demonstrate that they voted as instructed. Voter secrecy helps guard against vote buying schemes by prohibiting issuance of a vote receipt. According to Shamos (2004) vote receipts could create an epidemic of vote-buying.

Paper ballots can be also be damaged or lost during transit. Maintaining electronic vote records can mitigate the impact of this risk. Secure ballot provides additional safeguards. In Alaska, by law, if ballots are lost, the state can mandate a new election.

Ballot printing mistakes can disrupt an election. Ballots need to be printed and cut according to strict equipment vendor specifications so that they can be fed smoothly into the AV-OS machines and read accurately without jamming. Ballot printing is a specialized process. Mistakes could prevent accurate ballot insertion and vote counting, perhaps on a state-wide level. To date, there have been no reported issues relating to the physical attributes of the ballots from the current ballot printer. The current ballot printer used by the state has proved to be reliable and accurate. For their elections, most boroughs and municipalities also contract with the same ballot printer[8] that Division of Elections uses.

[8] Boroughs that don't use Print Works send their ballots out-of-state to Premier to print their ballots.

Recommendations:

2008 Election Cycle:

Maintain current relationship with Print Works in Homer. There are not a lot of people in the country who can consistently and accurately produce ballots that comply with the AccuVote system. Ballot printers for ballots used with AV-OS systems must be certified to Premier standards. The recent move of many states to paper ballots is pushing the capacity of the current printing infrastructure.

Post Election:

This system works very well at present. However, since there is not another qualified in-state ballot printer alternative, it would be beneficial to identify a qualified back-up.

Section 1.11 – Security Vulnerability Matrix

Description:

Summarize the security vulnerabilities of the equipment and procedures. To the extent possible, demonstrate the level to which proposed enhancements (equipment and procedures) mitigate security risks.

Summary of Analysis:

The intent of the security vulnerability matrix is to convey the major findings of Phase 2 in a clear, concise manner. The matrix presents the findings in terms of two parameters. See Appendix R - Master Matrix: Recommendations, Risk and Value Assessment.

Risk represents a qualitative estimate of the risk level associated with each item in the Phase 2 project scope. Risk is shown on a three level scale of high, moderate and low. The risk value assigned for each item is not a measureable quantity but rather an aggregation of information obtained during research conducted throughout Phase 2. High risk items are intended to identify areas where focus should be immediately applied. Moderate risk items identify areas requiring attention which should be addressed within a reasonable period of time. Low risk items offer little or incremental increase in performance.

Value represents the amount of benefit obtained by executing a recommendation. Value is rated on a scale of one (lowest) to three (highest). Items with the highest value represent good investments of labor and material resources. The benefit obtained by high value recommendations result in a reduction in component or overall system risk. Items with values of one or two represent investments which may require further research or justification. Clearly, low value, low risk items should be carefully studied before financial investment is made to ensure that implementation of the recommendation makes sense.

The matrix provides a series of columns which describe each scope item (consistent with the Phase 2 scope) and a risk associated with the current system implementation. Additional columns represent recommendation execution value and residual risk remaining following the execution of a recommendation. Resource and time constraints do not allow the Division of Elections to execute all of the suggested recommendations prior to the 2008 election cycle. As such a further set of columns represents the value and residual risk associated with implementing recommendations following the 2008 election cycle. Finally, a column is provided which provides constraints, limitations or notes associated with an individual scope item.

In addition to the matrix provided, a graphical representation of the current (2008) election cycle and the future election cycle scope items is provided. The purpose of these figures is to provide a fast, easy method to interpret the results in the matrix. A grid of 9

boxes represents the current value of risk for each scope item. Presence of a box with the scope items task number in a grid cell indicates its risk and value. The color (black, gray, white) represents the residual risk remaining if the recommendations provided are implemented

Section 1.12 – Security Training

Description:

Develop security training procedures that can be included as an addendum to existent training documentation.

Summary of analysis:

Poll workers represent one of several layers of defense in depth to help observe and guard against tampering. Currently Alaska poll worker training material does not include any security training. Not all of Alaska's poll workers attend training sessions. We reviewed and collected training documents from other election jurisdictions including California counties, Florida, Georgia, Indiana, Maryland, Mississippi, Missouri, New Hampshire, New York City, Ohio, and Wisconsin. Other research shows that better poll worker training is associated with increased voter confidence (Pew Center on the States, 2007). Weiser and Goldman (2007) recommend uniform statewide training.

Recommendations:

2008 Election Cycle:

We recommend training and checklists that will increase poll worker awareness of the possibility of attacks. Training which reminds poll workers of the importance of vigilance and secure equipment storage is part of building a multi-layer defense in depth election security system. It is also important to be alert to unusual and suspicious situations. For example, one such attack might be an attempt to divert poll workers attention to a false emergency. Another might be a disruption that could cause a massive denial of service. These kinds of disruptions are most likely in close races, in precincts where a candidate expects to lose.

We also recognize that poll workers are temporary employees and have a responsibility to not impede elections. Election crimes include causing eligible people to be excluded from elections, eligible votes not to be cast or counted, or other interference with election results (EAC 2006). It is important for poll workers to maintain the delicate balance between security and facilitating voting for all eligible voters.

We recommend training poll workers to inspect tamper evident seals.

We recommend that the Division of Elections provide more specific instructions how to "store your ballots, optical scan unit, and touch-screen voting unit in a secure location" in training (State of Alaska 2006). Refer to Appendix H - Security Training for more information.

Post Election:

Suggested changes to poll-worker training include enhanced security procedures as well as use of more effective training methods. The Division of Elections should consider implementing on-line training programs in addition to in-person training sessions. Consider certification and/or increase in poll-worker pay tied to successful completion of training. Poll worker wages are currently set by state statute so increases in wages would require legislative approval.

Part 2 Fortification of Systems

Description:

Section 2.1 Assess the integrity of the hardware and software of the electronic voting systems and their ability to accurately tabulate and report results.

Section 2.2 Evaluate communication protocols and make recommendations regarding data transmittal to GEMS to avoid the introduction of viruses and longtime delays in election returns.

Section 2.3 Evaluate the reliability and accuracy of the optical scanning and touch screen systems and their ability to function properly in Alaska weather and transportation/handling conditions. Study existing Premier reliability testing levels and equipment maintenance procedures to identify any concerns

Summary of Analysis:

The AccuVote election system is made up of voting components which are physically distributed across the State of Alaska. The AV-OS and AV-TSX voting machines are used to capture and tally votes within individual precincts. Six GEMS servers are also used during an election to enter hand-counted paper ballots on election night. The AccuVote system allows the election administrators to tabulate preliminary, unofficial results rapidly by transmitting the results stored in memory cards from each AV-OS and AV-TSX machine to a GEMS server in Juneau where the preliminary results are tabulated on a statewide level.

The current election system is implemented using a single director's office GEMS server which is used for both election programming and preliminary vote tabulation on the night of the election. AV-OS memory cards are programmed in the Juneau director's office using an AV-OS machine connected to the director's office GEMS. This machine is responsible for programming all of the AV-OS memory cards for the election state-wide.

The transmission of each AV-OS and AV-TSX machine's results is performed using a built-in analog modem. The network of analog modems is connected to the public switched telephone network at each precinct using a standard telephone jack. The AV-OS and AV-TSX modems dial a bank of 48 analog modems in the Division of Elections director's office in Juneau, Alaska. The modems establish a communications channel between the voting machine (AV-OS or AV-TSX) and the GEMS server in Juneau. The GEMS software incorporates a communications security feature called secure socket layer (SSL) which encrypts the data transmitted over the modem channel. The Division of Elections operates the communications channels with this feature enabled reducing the likelihood of an eavesdropping attack. At no time is the internet used for communication of or transmission of results.

Appendix J – AccuVote Communications System Description and Appendix K – AccuVote Network Topology provide a system description of the AccuVote communications system. The network schematic provides an overview of the connectivity between each region and the GEMS server in Juneau.

The State of Alaska requires paper ballot as the ballot of record (AS15.15.030 and AS15.15.032). The implementation of this paper ballot in Alaska relies primarily on optically scanned ballot cards which are filled out by each voter. This system has an inherent redundancy which allows a hand count in the case of a total system failure. Although the likelihood of a total system failure is very low, this redundancy ensures that no election will be conducted in which a voter would be unable to cast a ballot at any precinct.

Premier offers an application - Key Card Tool - which is designed to increase the security of AV-TSX memory cards and access cards. The Key Card Tool application allows the Division of Elections to change the passwords and encryption keys on the central administrator, supervisor, and voter access and memory cards. Current passwords and encryption keys are available in the public domain and cannot be considered secure.

Recommendations:

The SOAESP project team did not identify any vulnerabilities requiring remediation in the implementation of the AccuVote communications system. The implementation in use by the Division of Elections is robust and reasonable. It is important to note that all results provided to the public through the transmission of election results are preliminary and must be considered unofficial.

2008 Election Cycle

We recommend implementing the Premier Key Card Tool application to improve the security of the memory cards used in the AV-TSX machines.

We recommend using a GEMS server system that implements the Air Gap Management model (See Appendix M – AccuVote Functional Test Guidelines).

We recommend dedication of a single purpose AV-OS machine for programming AV-OS memory cards in the director's office.

Post Election

Empirical failure data provided by the Division of Elections point to shipping damage as a cause of some hardware failures in the AV-OS machines. It is recommended that improved shipping containers be used to reduce machine stress during transportation. We recommend using secure transport cases, similar to Pelican™ Products 1600 series cases, for transporting AV-OS machines. These cases add a layer of protection against tampering as well as guarding against weather and rough handling. Cases should be locked or sealed. See Appendix I – AccuVote OS Shipping Container Example.

Part 3 Confidence in Outcomes

Section 3.1 – Functional, Logic and Accuracy Testing

Description:

Evaluate processes and procedures the Division of Elections uses for functionality testing and logic and accuracy testing of systems and memory cards.

Summary of Analysis:

The AccuVote election system operated by the Division of Elections requires two different types of testing prior to each election to ensure reliable, error free operation. Functional testing refers to a suite of tests which validate the functional operation of each voting optical scan and touch screen voting machine. Functional testing is required to ensure that the machine will operate as designed on election day. The purpose of functional testing is to identify component failures or issues prior to deployment of the machine for use. Logic and accuracy testing refers to a suite of tests used to validate the error-free operation of the voting machines. The purpose of logic and accuracy testing is to ensure that the ballot programming is accurate and that voter intent is accurately represented in the resulting vote tallies. .

Appendix M is a set of functional test guidelines for the AccuVote system components. The appendix first outlines the functional tests currently implemented by the Division of Elections for each component. A set of recommendations to enhance the functional test suite is then presented. Although the Division of Elections currently performs a subset of the recommended tests it was found that improvements could be made in the test procedures by adding a number of additional tests and by improving the documentation of the test results.

Appendix N is a set of logic and accuracy testing guidelines for the AccuVote system components. The Division of Elections current AccuVote tests procedure can be made more rigorous by following the procedures provided Premier's *State of California: Use Procedures* document. This document provides a comprehensive list of recommendations for secure, error-free use of the AccuVote system. A subset of these recommendations which are applicable to the Alaska's system is outlined in the appendix.

Recommendations:

2008 Election Cycle:

We recommend that the Division of Elections adopt the increased scope of the recommended logic and accuracy test guidelines provided in Appendices M and N. Use of the enhanced procedures decreases the likelihood of an election day failure and reduces the probability of equipment logic or accuracy errors.

Post Election:

We recommend that testing technicians document procedures for revised functional test, logic and accuracy procedures.

We recommend that the guidelines presented in Appendices M and N be used to develop a long-term test documentation system whereby the results of each election cycle's functional, logic and accuracy test results are measured, validated and stored for later access and review.

Section 3.2 – Methods to Improve Voter Confidence

Description:

Identify methods that the Division of Elections can use to improve voter confidence.

Summary of analysis:

Other researchers determined that numerous factors influence public confidence in elections (Celeste, Thornburgh, Lin 2006, Weiser and Goldman 2007). Election administration processes and procedures can directly influence many of these[9] factors.

- Voters' personal experiences at polling places. Research shows that a voter's personal experience is closely related to the level of poll worker training. According to a Pew Trust report (Pew Center on the States 2007), poll worker confidence translates to voter confidence.
- Confidence in election equipment. Closely related to personal experience is voter confidence in election equipment. Most of the concern about election security involves touch screen systems including the AV-TSX machines used in Alaska. In Alaska, each precinct must have a mechanism in place for voters as mandated by the federal Help America Vote Act (HAVA). The AV-TSX touch screen voting systems meet the HAVA requirements. Each of these systems provides a mechanism that allows a voter to verify their individual vote. Additionally votes are recorded on a paper reel inside the touch screen unit that is later verified during a precinct level validation. This paper reel is considered the official paper ballot record. In Alaska, less than 1% of votes are cast on AV-TSX machines. In 2006, five communities used AV-TSX machines for all or most of their votes because these communities would otherwise require a hand-count of paper ballots. However, in most communities very few, if any votes are cast on AV-TSX systems. In Alaska's 2006 general election, in 224 precincts no one used the AV-TSX machines. In 112 precincts, fewer than five voters used the machines.
- Transparency. Alaska has an open process in which observers are encouraged to participate in and observe the entire voting and auditing process. Election procedures are uniform across the state and are written into state statute.
- Availability and frequency of recounts. Alaska has had many close races and frequent recounts. In Alaska, a vote margin less than or equal to 0.5% fewer than 20 votes triggers a recount. Otherwise a candidate or group of ten or more voters may request a recount. The candidate or proposition with the most votes in a

[9] Factors that are beyond the direct influence of election administration procedures are: faith in specific public officials, trust in democratic process, lack of public controversy around election administration, broad acceptance of election systems by social elites, substance and tone of election and political rhetoric, voter technological literacy and knowledge, and election outcome

recount is declared the winner. Since Alaska started using AV-OS machines in 1998, there has never been a case when the recount results changed the election outcome.

- Management of elections by non-partisan elections officials. With the exception of the director of the Division of Elections, Alaska's election officials are employees hired through the state employment process. Most have been working on elections for a long time. We found that several people had tenures of almost 20 years. Regional directors report that many poll workers have long tenures as well.
- Post election audits. The purpose of post-election audits is to give the public confidence that the election machinery is counting votes correctly. The Division of Elections conducts a post election audit, with bi-partisan participation and observers present.
- Paper ballot as the official ballot. According to Alaska state statute, the paper ballot is the official ballot (AS15.15.30 and AS15.15.32). Alaska is one of 35 states that require some form of paper back up. Of the 29 states, 13 use the paper ballots to audit results from electronic tallies (Pew Center for the States 2008, VerifiedVoting.org 2008).

Recommendations:

2008 Election Cycle:

Poll workers need to ensure that if one person uses an AV-TSX machine, at least five voters use it. At least 5 voters need to AV-TSX to protect voter confidentiality. Use the Division of Elections website to encourage members of the public and people concerned about the election system to become observers, encourage people to become poll workers and to make results of this evaluation accessible to the public.

Post Election:

We recommend that the Division of Elections expand its efforts to recruit poll workers and election observers, use the Division’s website and media to inform the public about Alaska’s election system, consider working with high schools to develop a module for teaching about Alaska’s election system and recruiting high-school students to work as poll workers.

Section 3.3 – Metrics and Continuous Improvement

Description:

Establish metrics that the Division of Elections can use as part of a procedure to demonstrate continuous improvement effort regarding of election security and predictability of results over time.

Summary of Analysis:

Sustaining Division of Elections confidence is more likely if a Continuous Process Improvement (CPI) program is instituted. CPI is a structured approach to analyze and identify process improvement opportunities and institute improvements on a continual basis. In the case of the of the voting process, there will always be a need to have, in place, a systematic approach for keeping all levels of the organization involved in changes. The objective would be to keep the staff, equipment, software, procedures and training up to date. An important aspect of CPI is the requirement for criteria to be identified and measured. Measurement becomes the source of metrics on which improvement is based. Throughout the voting cycle, there are opportunities for procedures to collect metrics that, in turn, can be pursued for improvement.

CPI is commonly referenced throughout management and public administration literature and is considered an effective approach for keeping up-to-date and improvements a normal part of the organizational culture. CPI was developed first by Dr. W. Edwards Deming and initial referred to as the "Shewhart cycles". Continuous improvement is accomplished as an iterative cycle that repeats the following steps: Define – Measure – Analyze – Improve – Control. CPI was first applied to quality control in the manufacturing process. The approach is now adapted by many organizations (private and public) for the purpose of involving all organizational levels in improving the quality of services and keeping technologies current (Kelly, 2003; Xenakis and Macintosh, 2006).

An example of a possible criterion for consideration is: "Percent of pre-election testing errors". This is measurable and can be evaluated using a root-cause methodology and subsequent measures indicate improvements. Specific criteria are established as part of the improvement process and reflect the goals of Division of Elections.

The four election regions are not identical and there will always be differences regarding staff experience and voting challenges. There is a need to adopt a methodology within Division of Elections that allows for all of the staff to help in planning and in facilitating improvements in all aspects of the voting process. These include updates in software, equipment, training and related materials. Regional offices need to be involved both because of their contribution to the understanding of unique challenges in the various area of the state and the advantage of having the improvements integrated between regions. All regions improve because of their collective efforts.

Recommendations:

This is to be a change in managerial procedures intended to involve managers at all levels of Division of Elections and will take time to initiate and implement.

2008 Election Cycle:

Very little can be accomplished between now and the end of this election cycle however preliminary objectives, metrics can be explored. Consider conducting an audit during the election to evaluate if these preliminary criteria are the right metrics and use this to collect some baseline data.

Post Election:

Instituting a CPI program should be considered starting in 2009 beginning with overall training of the topics and process of CPI. Next is setting specific improvement goals and measurable criteria. Measurement of results is critical because this becomes the basis for measuring improvements.

We recommend that the regional directors play a role in CPI both because they are close to the unique challenges within the regions and also this involvement facilitates integrating and standardizing the improvements between the regions.

Section 3.4 - Public Input and Commentary

Description:

Provide a weekly review of emails from the public on security issues and summarize and publish general responses to them on the Division of Elections website.

Summary of Analysis:

From September 2007 through end April 2008, six emails were received from members of the public. The suggestions in the emails included:

- Use punch cards that could be fed into an optical scanning system for tallying.
- Hand-count all ballots in the next election.
- Use two-part ballot that would provide a receipt showing the votes cast.
- Eliminate touch screen systems.
- Provide a tear tab with a serial number. Voter could later visit a website to verify correct vote recording using serial number.
- Post results through a website as votes are tallied.
- Set optical scanner to read fainter marks to ensure all legitimate votes can be counted.

Only systems that have been certified by the Election Assistance Commission (EAC) Voting Systems Standards can be used in federal elections. These specifications include detailed requirements pertaining to functional capabilities, hardware standards, software standards, telecommunication standards, security standards, quality assurance standards and system configuration management. Each system certified by the VSS must pass a set of tests performed by an Independent Test Authority (ITA) that has also been certified by the EAC. These standards also include detailed information about ballots and accessibility for voters covered by the American with Disabilities Act (ADA) and HAVA. Currently, by law, systems used in Alaska must conform to the VSS 2002 standard. As new capabilities are developed by election equipment vendors, this equipment must be certified to this minimum standard as well as any then current standard required by law.

At this time, there are no punch card systems that are certified to the VSS standard. Random hand-counts and requests for hand counts for close elections help ensure vote counting accuracy. Election results have never changed as a result of random hand-counts and mandatory or requested recounts.

To protect voter privacy, receipts are not issued. The internet is not considered a secure mechanism for transmitting voting results. At this time, memory cards containing the votes cast on each machine are manually inserted into centralized vote tabulation machines. Real-time information about vote tallies is not provided to ensure that no election results are posted prior to the conclusion of the election. For more detailed

information on the reliability and accuracy of the optical scanning system please see Appendix L – AccuVote Reliability Assessment.

The suggestion to implement a system of tear tabs with serial numbers refers to using cryptographic methods to verify votes. The voter receives an encrypted copy of their voted ballot with a randomized serial number. Voters can use the serial numbers to get internet access to a decrypted version of their voted ballot (Robinson 2004, 2004b). Implementing this process would involve a different system than what is in place. It is one of several innovations worth considering in the event of an overhaul.

2008 Election Cycle:

Continue to monitor feedback through Division of Elections website and respond to frequently asked questions.

Post Election:

Continue to monitor feedback through Division of Elections website. Incorporate suggestions into continuous improvement process (CIP).

Section 3.5 – Absentee Ballot Process

Description:

Provide a description of the absentee ballot process.

Summary Analysis:

Absentee voting is a major component of the election process because, in the last election, 19% of voters voted by absentee. There are two broad categories of absentee voting. The first category includes absentee by mail, fax and special advanced requests. The second category is called "in-person absentee" It includes special needs voting, early voting and absentee in person voting.

In all cases, the process starts with the Division of Elections' request for ballots to be printed. Absentee ballots are produced as part of the same purchase order to the printer order for precinct voting ballots. It is placed 48 days before the election. The ballots are numbered in sequence with numbers of ballots printed from estimates based on previous elections. State of Alaska statute requires that all absentee ballots be reviewed, opened and counted by the 15th day after the election. Absentee ballots are not part of the post-election audit process.

Absentee voting information is detailed on the State of Alaska, Division of Elections web site and procedures for the various categories are outlines in: Absentee Voting Station Official Procedures (Rev. 5/2006) and Absentee Voting Official's Handbook (Rev. 4/25/06). Regarding both categories of absentee voting, the Division of Elections has carefully delineated the open period for the respective absentee voting as well as the process and procedures for voting absentee. We identified one issue unique to absentee voting that requires special attention: *time exposure*. The ballots are in distribution, storage and most importantly, in use, over many more days than the ballots and machines used specifically at a polling place on election day.

Appendix Q - Summary of Absentee Voting delineates types of absentee voting and respective pre- and post-election dates of the process.

Recommendations:

2008 Election Cycle:

All of the security issues with regard to memory cards, upgrades and ballots used at polling places for election day also apply to absentee voting. Ballots stored for use in absentee voting need to have tight security to avoid loss, damage or tampering along with procedures and staff training emphasizing the risks of unauthorized access. Procedures for "end-of-day" documentation, distribution, ballot storage and shipping, and final

delivery of ballots and reports to Division of Election in Juneau need special attention to assure adequate control and accountability (see Appendix H – Security Training).

Post Election:

The voting equipment used in support of the absentee voting processes should be identified in general usage/maintenance records should the need arise to assess unusual usage, security concerns and/or maintenance patterns.

Section 3.6 – Random Sampling Methodologies

Description:

Research other random sampling methodologies that might provide additional confidence in election results. These recommendations would be proposed for further consideration and evaluation.

Summary of analysis:

Random sampling methodologies refer to sample size and how ballots are chosen for hand counts in Alaska's post election audit.

The main purpose of the post election audit is to increase public confidence in election results. Audits do this by verifying that the machine counts were correct and confirming that a manual recount would not change the outcome. Audits also detect tampering with the system, detect large scale systemic errors, deter fraud, and provide feedback to allow jurisdictions to improve voting technology and election administration (Norden 2007). The random sample should be large enough to be able to detect discrepancies but small enough to be efficient so that hand counts don't take a long time. Alaska is one of only 12 states with an election audit (Norden 2007) program. Many states are currently evaluating and pilot testing audit procedures and sampling methods. But to date, there is little agreement about which is the best audit procedure (Norden 2007).

One of the benefits of a uniform statewide system in Alaska is that observers only need to go to one place to see the audit. Alaska's random selection process is transparent. Bi-partisan review board members select the random sample by drawing precinct numbers from strips of paper in a box. Precincts are eligible for selection if they include at least 5% of the voters in that House district. In Alaska, a bi-partisan review board hand counts ballots from one precinct in each house district. If the results of the hand count differ from the results from electronic counts by more than 1%, all ballots in that House district must be hand counted. To date, there has never been a case where counts differed by more than 1% in any precinct.

Recommendations:

2008 Election Cycle:

No changes this year.

Post Election:

Wait to consider changes until audit evaluations in other states are finished. Any changes to the procedure would require legislative approval since the audit procedure is written into Alaska state statutes.

Conclusions

The following table summarizes our main recommendations, some of which the Division of Elections could put into effect before the August primary and the November general election, and some of which it can't.

Recommendations for Improving Alaska's Election Security

Change By 2008 Election	Why?	Change After Election	Why?
✓ *Verify the accuracy of voting technology before and after the election, by comparing code in voting machines with correct, registered code* ✓ *Install new software that allows election officials to create a more-secure password authentication system for touch-screen machines* ✓ *Change passwords on all voting technology throughout the system* ✓ *Use tamper-evident seals on shipping cases and envelopes* ✓ *Add election-security material to poll workers' training manual* ✓ *Increase vigilance about security procedures in absentee polling locations* ✓ *Purchase state-owned voting machines for use in North Slope Borough, rather than borrowing borough-owned machines*	This series of changes in technology and election procedures will make the existing technology more secure; improve security procedures among election officials and poll workers; and help increase Alaskans' confidence in the integrity of state elections. These measures can all be taken in the short-term, before the August primary and the November 2008 election.	✓ *Upgrade voting machines and other technology to new, improved platform* ✓ *Establish long-term security goals and a method for measuring progress* ✓ *Improve testing processes to insure all voting technology is functioning properly and recording votes accurately* ✓ *Develop and implement a standard plan for tracking and changing passwords* ✓ *Improve system for tracking the number and location of voting machines, through bar-codes or other inventory-control measures* ✓ *Strengthen storage facilities for voting machines and other system components with dead-bolt locks, alarms, ceiling grids, self-locking doors, and other features to prevent forced entry* ✓ *Buy more-secure shipping containers for optical-scanners* ✓ *Recruit and train more poll workers* ✓ *Consider partnerships with other institutions to do ongoing evaluation and implementation of changes in election-security technology*	Installing the new platform is the single-most important change the state can make, because it will reduce or eliminate risks of vote-tampering identified in the current system. But the platform must first be certified to the Election Assistance Commission's 2002 Voting System Standards, and after that will require an estimated 1,000 man-hours to install on election equipment statewide. Even if it were certified soon, it is not practical now to install the upgrade before the 2008 elections, given the time, expenses, and logistics involved. The other post-election recommendations are either longer-term enhancements of measures recommended for 2008, or additional security measures that there isn't time enough to implement before the 2008 elections.

- Upgrade to the new, more secure platform after the election. We can't over-emphasize the importance of this upgrade. Alaska, California, Florida, and other states use the same or similar voting technology. Election-security studies in several states found that the existing technology was potentially vulnerable to vote-tampering in a number of ways. The new platform, Premier Election Systems Assure 1.2, which the manufacturer developed in response to those studies, is still being tested to insure that it meets standards set by the federal Election Assistance Commission. We had hoped the system could be installed on Alaska's voting equipment by the 2008 election, but we now believe that's not feasible. Alaska is now in the run-up to the August primary and the November election. The Division of Elections is programming its equipment for those elections and doing other work that has to meet specific pre-election deadlines. Also, because the state shares voting equipment with local governments, the upgrade will have to be coordinated with them as well. To add it is a huge, expensive job requiring complicated logistics at this point is not feasible. But we recommend that it be done as soon as possible after the election.
- Establish security goals and a method for regularly measuring progress toward those goals. The Division of Elections is well aware of security issues, and has taken a number of steps to improve security. But it currently has no long-range security goals, nor a plan for measuring progress. We believe it's very important for the division to develop such goals and systematically meet them.
- Consider forming a partnership with some other organization that could continuously monitor and evaluate any new election-security vulnerabilities and ways to improve security. This would allow the Division of Elections to quickly make any necessary changes or improvements, before problems developed. Some states are already doing this. The Division of Elections itself does not have adequate staff to do such monitoring.
- Install new software that allows election officials to create a more-secure password authentication system for touch-screen machines. Election officials are in fact already installing this new software, as they do programming for the upcoming election. This new software, called Key Card Tool, allows them for the first time to create their own authentication password and encryption keys for the state's 439 touch-screen machines. This is a substantial improvement in security. Previously, the default password and keys were in the public domain. They were programmed into all the touch-screen machines and couldn't be changed. Now, the password and keys can be changed regularly, and over time election regions could have their own individual passwords and keys.
- Verify the accuracy of voting technology. Before and after the November election, election officials should test all voting machines by comparing code in the machines with correct, registered code. In the longer-term, the state should develop standard testing processes to insure all voting technology is functioning properly and recording votes accurately.

- Change system passwords. Before the election, the state should change all passwords currently used in election-system technology. After the election, the state should develop a plan for routinely tracking and changing passwords.
- Use tamper-evident seals on envelopes and shipping containers. This precaution can be taken before the upcoming election. Critics argue that attackers could in fact open such seals without leaving any evidence of tampering. But we believe that especially in Alaska—where ballots and equipment can travel long distances under difficult conditions—tamper-evident seals do help improve security.
- Recruit more poll workers and improve their election-security training. Before the election, the Division of Elections should add a section on election-security to the existing training manual, which doesn't currently discuss security. In the longer term, the state needs to recruit more poll workers—which in itself would help improve security in polling places—and to provide better training (possibly online) in election-security procedures.
- Improve the way voting machines are transported, tracked, and stored. Most of these recommended improvements can't be made until after the November election. They include buying better shipping containers for optical-scan machines, which have to be shipped to many small communities from larger regional centers before and elections and returned afterward. The state also needs a better system for tracking the number and location of voting machines, through bar-codes or other methods of inventory-control. Also, the physical security of machines in storage needs improvement. The state should consider reinforced doors, dead-bolt locks, ceiling grids, alarms, and other measures as appropriate.

We have made a number of recommendations for improving the security of Alaska's election system, but we want to keep those recommendations in context: Alaska's election system is in good shape. Other states are now adopting measures we've had in place for years. Personnel of the Division of Elections understand the system and have a good idea of what kinds of measures could help make it more secure.

But there's always room for improvement. Aside from the specific recommendations we've listed, Alaska needs to build a foundation for the future—to make sure Alaska's election system stays among the best in the country. The current election technology is aging, and the state will face new choices when it has to upgrade that technology. It needs to start systematically assessing its future needs and new technologies now.

Proposed Statement of Work for Phase 3: Implementation

1. Investigate Institutional Partnership
2. Develop revised functional, logic and accuracy testing procedures
3. Continue to monitor poll-worker training and auditing programs going on in other states (grant-based work being done) including on-line training capabilities.
4. Develop Assure 1.2 upgrade procedure.
5. Perform Assure 1.2 cost benefit analysis for implementation methodology
6. Design process to audit use of and results from implemented recommendations.
7. Develop procedures for recommended technical enhancements (e.g. hash code)

References

Alvarez, R. Michael & Hall, Thad E. (2005, June). *Public attitudes about election governance*. University of Utah, Center for Public Policy and Administration and Caltech/MIT Voting and Technology Project.

Alvarez, R. Michael. (2005, October 5). *Precinct voting denial of service*. Paper prepared for NIST (National Institute of Standards and Technology) Threats to Voting Systems workshop. Caltech-MIT Voting Technology Project.

Bishop, Matthew. (2007). California red team review of Diebold voting system. *State of California Top-to-Bottom Review.*

Calandrino, Joseph A., Feldman, Ariel J., Halderman, J. Alex, Wagner, David, Yu, Harlan, Zeller, William P. (2007, July 20). *Source code review of the Diebold voting system.*

California Secretary of State. (2007, October 17). *Withdrawal of approval and conditional reapproval of Diebold Election Systems, Inc. GEMS 1.18.24/AccuVote-TXS/AccuVote-OS DRE and optical scan voting system.*

California Secretary of State. (2007, October 25). *Post-election manual tally requirements.*

Celeste, Richard, Thornburgh, Dick, & Lin, Herbert (Eds.). (2006). *Asking the right questions about electronic voting.* Washington, DC: National Academies Press.

Diebold Election Systems. (2007, August 22). *Report of Diebold Election Systems, Inc. (DESI) to California Secretary of State Red Team report issued on the GEMS 1.18.24/AccuVote-TSX/AccuVote-OS/DRE & optical scan voting system.*

Diebold Election Systems. (2004). *GEMS 1.18 product overview guide* (Revision 2.0).

Diebold Election Systems. (2005). *AccuVote-TSX ballot station 4.6 user's guide* (Revision 2.0).

Diebold Election Systems. (2005). *AccVote-OS Precinct Count 1.96 user's guide* (Revision 4.0).

Diebold Election Systems. (2005). *GEMS 1.18 user's guide* (Revision 12.0).

Diebold Election Systems. (2006). *Verifying EPROM program file versions for the AccuVote-OS product* (Revision 2.0).

Diebold Election Systems. (2007, January 11). *Client security policy* (Revision 6.0).

Diebold Election Systems. (2007). *Key card tool 4.6 user's guide* (Revision 4.0).

Diebold Election Systems. (n.d.). *Response and solutions to system review recommendations*.

Diebold Election Systems. (n.d.). *Verifying GEMS hash key quick reference guide.*

Gardner, R., Yasinec, A., Bishop, M., Kohno, T., Hartley, Z., Kerski, J., et al. (2007). *Software review and security analysis of the Diebold voting machine software.* Florida State University, Security and Assurance in Information Technology Laboratory.

Johnston, Roger G. (2006, Nov-Dec). Tamper-indicating seals. *American Scientist, 1*. p 515-523.

Kiayias, Aggelos, Michel, Laurent, Rusell, Alexander, Shashidhar, Narasimha, See, Andrew, Shvartsman, Alexander, et al. (2007, December). *Tampering with special purpose trusted computing devices: A case study in optical scan e-voting*. Paper presented at the 23rd Annual Computer Security Applications Conference, Miami Beach, Florida.

Kuo, C., Romanosky, S., & Cranor, L. (2006). Human selection of mnemonic phrase-based passwords. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS '06)* (pp. 78-78). Pittsburgh, PA: ACM Press.

Norden, Lawrence D., & Lazarus, Eric. (2007). *The machinery of democracy: Protecting elections in an electronic world*. Chicago: Academy Chicago Publishers.

Pew Center on the States. (2007, September). *Helping Americans vote: Poll workers*.

Pew Center on the States. (2007). *The Help America Vote Act at 5*.

Premier Election Solutions. (n.d.). *Premier master equip acceptance test procedures 012008.xls*.

Premier Election Solutions. (2007). *Plan on formatting and clearing program storage on Voting System* (Revision 1.0).

Premier Election Solutions. (2007). *Premier's Windows configuration guide* (Revision 3.0).

Premier Election Solutions. (2007). *State of California use procedures*.

Premier Election Solutions. (2008). *AccuVote-OS hardware guide* (Revision 13.0).

Premier Election Solutions. (2008). *AccuVote-TSX hardware guide* (Revision 13.0).

Premier Election Solutions. (2008, January 17). *California tamper evident security seal document* (Version 2).

RABA Technologies LLC. (2004, January 20). *Trusted agent report, Diebold AccuVote-TS voting system*. Retrieved March 21, 2008 from http://www.raba.com/press/TA_Report_AccuVote.pdf.

Rausand, R., & Hyland, A. (2004). *System reliability theory: Models, statistical methods, and applications* (2nd ed.). Hoboken, NJ: John Wiley & Sons, Inc.

Robinson, Sarah. (2004, March). What's so special about voting? *SIAM (Society for Industrial and Applied Mathematics) News, 37* (2).

Robinson, Sarah. (2004, April). Works in progress: trustworthy cryptographic voting systems. *SIAM (Society for Industrial and Applied Mathematics) News, 37* (4).

Shamos, Michael Ian. (1993). *CFP'93 Electronic voting--evaluating the threat*. Retrieved October 15, 2007 from http://euro.ecom.cmu.edu/people/faculty/mshamos/CFP93.htm

Shamos, Michael Ian. (2004). *Paper v. electronic voting records—an assessment*. Retrieved October 15, 2007 from *http://euro.ecom.cmu.edu/people/faculty/mshamos/paper.htm*

Spafford, E. (2006, April 19). *Security myths and passwords*. CERIAS (The Center for Education and Research in Information Assurance and Security). Retrieved March 21, 2008 from http://www.cerias.purdue.edu/weblogs/spaf/general/post-30/

State of Alaska, Division of Elections. (2007). *Accu-Vote security enhancements and features.*

State of Alaska. (2006). *Alaska Statutes. Title 15: Elections*. Charlottesville, VA: Matthew Benders & Company, Inc.

State of Alaska. (2006). *Polling place election procedures. Hand count and* touch screen precincts.

State of Alaska. (2006). *Polling place election procedures. Optical scan and touch screen precincts.*

State of Alaska, Division of Elections. (n.d.). *Closing the polls, Accu-Vote optical scan unit transmitting results.*

State of Alaska, Division of Elections. (n.d.). *LAT testing and memory card preparation instructions.*

State of Alaska, Division of Elections. (n.d.). *Pre-Election cycle optical scan functionality testing.*

State of Alaska, Division of Elections. (n.d.). *Regional AccuVote board LAT report log.*

State of Alaska, Division of Elections. (n.d.). *Regional AccuVote board touch screen logic and accuracy test early voting memory card – general election.*

State of Alaska, Division of Elections. (n.d.). *Regional AccuVote board touch screen logic and accuracy test early voting memory card – primary election.*

State of Alaska, Division of Elections. (n.d.). *Regional AccuVote board touch screen logic and accuracy test precinct memory card – primary election.*

State of Alaska, Division of Elections. (2006). *Specifications for Division of Elections ballot transportation and security for the 2006 general elections.*

State of Missouri, (2007). *It's your turn: be a poll worker – 2007 survey results*.

Technical Guidelines Development Committee. (2007). *Voluntary Voting System guidelines recommendations to the Election Assistance Commission.* Technical Guidelines Development Committee.

Thompson, Clive. (2008, January 6). Can you count on voting machines? *The New York Times.*

U.S. Election Assistance Commission (EAC). 2006. *Election crimes: An initial review and recommendations for future study*. Washington D. C.

U.S. Federal Election Commission. (2002). *Voting system standards, Volume I: performance standards.* Washington, DC:

Weiser, Wendy R., & Goldman, Johan. (2007). *An agenda for election reform*. New York University School of Law, Brennan Center for Justice.

UNIVERSITY of ALASKA ANCHORAGE

State of Alaska Election Security Project

Phase 2 Report Appendices

Prepared for Lieutenant Governor Sean Parnell
and the State of Alaska Division of Elections

May 16, 2008
Final Report

This page left intentionally blank

Appendix A - Assure 1.2 Upgrade Labor Estimate					
Item Number	*Assure 1.2 Software or Firmware Component*	*Upgrade Procedure Description*	*Machines Affected*	*Estimated Hours Per Machine*	*Total Hours*
1	AV-OS Firmware Upgrade	Existing 1.96.6 firmware EPROM is physically replaced with 1.96.10 firmware EPROM. New EPROM to contain a serial number on bottom side of chip.	290	0.25	73
2	AV-TSX Bootloader Upgrade	Existing BLR 7.1.2.1 Bootloader software is upgraded to BLR 1.3.9	439	0.25	110
3	AV-TSX Windows CE Upgrade	Existing Windows CE operating system software is upgraded from the current version 4 10.2.1 to version 4 10.3.9	439	0.25	110
4	AV-TSX BallotStation Upgrade	Existing BallotStation software is upgraded from the current version 4.6.4 to version 4.7.2	439	0.25	110
5	AV-TSX AccuView Printer Module Software Upgrade	Existing AccuView printer modules software is upgraded from the current version model 3 rev. 3.03 to model A rev 3.03	439	0.25	110
7	GEMS Election Management Software Upgrade	Existing election management software is upgraded from the current version 1.18.24.0 to version 1.20.2	8	8	64
8	Key Card Tool Software Upgrade	The Key Card Tool software must be upgraded to version 4.7.1	2	8	16
9	Voter Card Encoder Upgrade	The voter card encoders must be upgraded from the existing version 1.3.2 to the Assure 1.2 version 1.3.3	1198	0.25	300
10	VC Programmer Software Upgrade	The VC Programmer software must be upgraded from the existing version 4.6.1 to the Assure 1.2 verion 4.7.1	System-level task	lot	4
11	Assure 1.2 Upgrade AV-OS Procedure Development	Develop and draft a plan and a procedure for upgrade of all AV-OS, AV-TSX and GEMS machines to include acceptance and functional testing following the upgrade procedure implementation.	System-level task	lot	100
				Total Hours	**995**

Appendix B - Assure 1.2 Upgrade Analysis

1. System Overview

The Premier Election Solutions AccuVote system used by the State of Alaska Division of Elections (DoE) is comprised of several different software and hardware components. These software and hardware components interact at different times during an election in order to allow election officials to prepare ballots and races, to allow voters to cast ballots and to allow election officials to tabulate the results of the election.

The State of Alaska DoE utilizes the following Premier system components in its implementation of the AccuVote election system.

1.1 AccuVote Optical Scan Model B (AV-OS)

The AccuVote Optical Scan (AV-OS) hardware is available in two different firmware configurations, precinct count and central count. The State of Alaska DoE does not use the Premier Election Solutions central count firmware.

The precinct count firmware version of the AV-OS is used by individual precincts to conduct elections and tally votes. The firmware in each AV-OS machine is stored on an Electrically Programmable Read Only Memory (EPROM) device which is accessed by the AV-OS hardware. The system utilizes a re-writable 40-pin Epson memory card to program individual elections. Tallied votes and ballot definition files are stored on the memory card. A precinct AV-OS machine reads the election mode from the memory card and adopts that functional mode for operation.

The firmware revision currently present on the AV-OS platform operated by the State of Alaska DoE is precinct count 1.96.6.

1.2 AccuVote Touchscreen Model D (AV-TSX)

The AccuVote Touchscreen (AV-TSX) hardware used by the State of Alaska DoE is a Direct Recording Electronic (DRE) machine with an additional module which produces a Voter Verifiable Paper Audit Trail (VVPAT). The AV-TSX machine allows voters to cast their votes from an electronic touchscreen interface. Once the ballot is cast the touchscreen device sends the ballot to a VVPAT printer where the voter validates the results. Once the voter accepts the printed ballot the vote is considered cast and the tallies are updated on the electronic memory card.

The AV-TSX machine requires two different applications to run. The bootloader application is used to load the Windows CE operating system image from the system flash memory. The State of Alaska DoE currently uses Bootloader v.BLR 7.1.2.1. The system also requires the BallotStation application which runs under the Windows CE operating system. This application implements the voter interface and administrative functionality within the AV-TSX machine. The State of Alaska DoE currently uses BallotStation v.4.6.4.

An additional security enhancement is available from Premier Election Solutions for use with the AV-TSX machines. The security enhancement is called Key Card Tool. Key Card Tool is

a software application which allows election officials to change encryption keys and access passwords within the AV-TSX system. The State of Alaska DoE is in the process of implementing the Key Card Tool application for the 2008 election cycle.

1.3 GEMS (Global Election Management System)

The Division of Elections utilizes a total of eight (8) GEMS servers distributed across the State of Alaska. The GEMS servers implement the ballot definition, vote tabulation and system reporting functions for the Premier Election Solutions AccuVote system.

Currently, the Division of Elections is operating identically configured Dell PowerEdge Servers which run the Premier Election Solutions GEMS applications.

The GEMS systems are running Election Management System v.1.18.24.0

In addition to running the Election Management System software, the system is operating with Dell BIOS A09.

The Division of Elections does not currently calculate hash codes of the certified software running on the GEMS servers.

1.4 Assure 1.2 Components

The Assure 1.2 software / firmware upgrade is a complete system revision. This system revision is comprised of several different software and firmware components which must be loaded on to each hardware platform in order to obtain a complete system upgrade.

1.4.1 AV-OS Components

The AV-OS model B machines must be upgraded from the existing 1.96.6 EPROM firmware revision to the AV-OS Precinct Count Firmware version 1.96.10 (build date 10-01-2007).

1.4.2 AV-TSX Components

The AV-TSX model D machines must be upgraded from the existing Bootloader v.BLR 7.1.2.1 to the Assure 1.2 Bootloader v1.3.9 (build date 11-19-2007).

The AV-TSX model D machines must be upgraded from the existing Windows CE version v.4 10.2.1 to the Assure 1.2 v.4 10.3.9 (build date 1-19-2007),

The AV-TSX model D machines must be upgraded from the existing BallotStation v.4.6.4 to the Assure 1.2 BallotStation v.4.7.2 (build date 01-07-08).

The AV-TSX model D machines must have the AccuView Printer Module software updated from AVPM model 3 Rev 3.03 o the Assure 1.2 AVPM model A v.3.03 (build date 11-01-07).

1.4.3 GEMS Components

The GEMS Servers must be updated from the existing Election Management Software v.1.18.24.0 to the Assure 1.2 v.1.20.2 (build date 11-19-2007).

The GEMS Servers must be updated to the Assure 1.2 Security Manager v.1.0.5 (build date 01-15-2008).

1.4.4 System-wide Components

The AV-OS model B machines and the AV-TSX model D machines must have the AccuBasic Report Files version updated to v.2.2.3 (build date 11-19-2007).

The Keycard Tool software must be updated to Assure 1.2 Keycard Tool v.4.7.1 (build date 11-01-2007).

The Voter Card Encoder must have the existing software v.1.3.2 updated to the Assure 1.2 Voter Card Encoder v.1.3.3 (build date 11-01-2007)

The VC Programmer must have the existing software v.4.6.1 updated to the Assure 1.2 VC Programmer v.4.7.1 (build date 11-01-2007).

1.4.5 Assure 1.2 Release Notes

At the time that this document was drafted the Premier Elections Solutions software had not yet been certified to the VSS 2002 standard. As such the Assure 1.2 release notes are not yet available for review.

2. Assure 1.2 Upgrade Cost Estimate

2.1 Assure 1.2 Software Cost Estimate

The State of Alaska Division of Elections has a current maintenance agreement with Premier Election Solutions, Inc. Software upgrades are provided to the Division of Elections at no additional cost while the maintenance agreement is in effect.

2.2 Installation and Validation Cost Estimate

The installation and acceptance testing of the Assure 1.2 upgrade represents a significant dedication of time by the Division of Elections. Upgrade from the existing AccuVote system revision to the Assure 1.2 revision requires the execution of ten individual tasks. A rough estimate of the labor hours associated with the implementation of each Assure 1.2 component is provided in “Appendix A – Assure 1.2 Upgrade Labor Estimate”.

3 Assure 1.2 Software Evaluation

Phase 1 of the SOAESP identified a number of different system issues presented by the California Source Code Review of the Diebold Voting System (Calandrino, et al. 2007), the California Red Team Review (Bishop, 2007), the Florida Software Review and Security Analysis of the Diebold Voting Machine Software (Gardner, et al., 2007) and others. As a result of this analysis, the State of Alaska is interested in evaluating Premier Election System's Assure 1.2 software release. This new release of software is applicable to the State of Alaska's AccuVote system.

The purpose of this section is to evaluate the Assure 1.2 software platform against the list of issues, vulnerabilities and problems identified in Phase 1. Recommendations are made regarding the installation of the Assure 1.2 on Alaska's AccuVote system.

3.1 VSS 2002 Compliance

The Premier Election Solutions Assure 1.2 is currently undergoing evaluation by the nationally recognized testing laboratory Systest. Premier Election Solutions, Inc. is confident that the Assure 1.2 software release will be compliant with the Voting System Standards 2002 certification requirements. Certification under the VSS 2002 requirements has not yet been received. State of Alaska law requires that the system be certified prior to installation on the production voting system.

3.2 California Red Team Review

The California Red Team Review (Bishop, 2007) identified a number of issues which are addressed by Premier in the Assure 1.2 platform. These issues are outlined below:

3.2.1 Precinct Count AV-OS Ballot Tampering

The California Red Team was able to verify previous results wherein the ballot totals in the AV-OS memory card could be tampered with to affect the outcome of an election.

The Assure 1.2 software release corrects this issue.

3.2.2 AV-TSX Malware

The California Red Team verified previous findings in which a malicious user might overwrite system firmware and / or software. The potential impact of this type of vulnerability was presented in the Red Team Report.

The Assure 1.2 software release corrects the bootloader issue. Premier believes that the format string error issue does not present a real vulnerability.

3.2.3 AV-TSX Escalation of Privileges

The California Red Team identified a vulnerability in which a malicious user might gain access to the system at the supervisor or central administrator level.

The Assure 1.2 software release corrects this issue. The user can still enter the system setup / diagnostics mode when a peripheral device failure occurs. Administrative functions are denied.

3.2.4 AV-TSX Default Static Key

The California Red Team commented in their report on the use of the default static authentication and data keys within the AV-TSX system.

The Premier Election Solutions Keycard Tool application should be used to increase the security surrounding smart card use in the AV-TSX system. Premier Election Solutions believes that Indication of the default key on the AV-TSX interface is a security feature. The Assure 1.2 software release updates the Keycard Tool application to version 4.7.1.

3.2.5 GEMS Databases

The California Red Team identified an issue with database access within the GEMS server where a malicious user could gain access to the GEMS databases and corrupt or manipulate the contents of the database.

The Assure 1.2 software release corrects the direct database direct read / write issue and improves database security.

3.2.6 GEMS Audit Logs

The California Red Team found that the audit logging functionality within the GEMS server was insufficient to identify all malicious user activity.

The Assure 1.2 software protects the election database using password access.

3.3 Florida Software Review

The Florida review team (Gardner, et al., 2007) identified a number of issues with the Premier Election Solutions hardware and software. The text below describes issues which were identified by the Florida team as requiring input and resolution by Premier Election Solutions.

3.3.1 RSA Hardware Signature Flaw

The Florida evaluation team found that the AV-OS and AV-TSX RSA encryption signatures which validate the AccuBasic scripts in the system firmware are implemented in a manner which is susceptible to malicious attack.

The Assure 1.2 software release corrects the hardware signature flaw.

3.3.2 AV-OS Memory Card Integrity Is Not Protected

The Florida evaluation team found that the AV-OS memory card contents are not encrypted or authenticated in any manner. This vulnerability was found to expose the AV-OS platform to attack.

Premier Election Solutions believes that a complete memory card authentication implementation is beyond the capabilities of the AV-OS hardware. Improvements relating to AccuBasic report scripts have been implemented. Physical memory card protection is recommended as a top security priority.

3.3.3 AV-TSX Cryptographic Key Management

Like the California Red Team, the Florida evaluation team found that the AV-TSX was vulnerable to smart card attacks when using the default data and security keys within the AV-TSX system.

The Premier Election Solutions Keycard Tool application should be used to increase the security surrounding smart card use in the AV-TSX system. The Assure 1.2 software release updates the Keycard Tool application to version 4.7.1.

3.3.4 AV-TSX Memory Card Update File is Unprotected

The Florida evaluation team found that the assure.ini file was not sufficiently protected within the AV-TSX system. This lack of protection was found to expose the system to malicious attackers.

The Assure 1.2 software release corrects this issue.

3.3.5 AV-TSX Smart Card Authentication Uses Only a Hard Coded Password

The Florida evaluation team found that even with the use of the Keycard Tool application the AV-TSX system was vulnerable to smart card attacks by skilled attackers.

Not addressed by the Assure 1.2 software release. Premier Election Solutions believes that the vulnerability identified in the Florida analysis can be satisfactorily mitigated by training election workers to identify and act on suspicious activity in the polling place.

3.3.6 AV-TSX Supervisor PIN is Not Cryptographically Protected

The Florida evaluation team found that even with the use of the Keycard Tool application the AV-TSX system was vulnerable to smart card attacks by skilled attackers.

Not addressed by the Assure 1.2 software release. Premier Election Solutions believes that the supervisor PIN is sufficient to protect supervisor access and that procedural checks should be implemented which restrict access to the supervisor cards.

3.3.7 AV-TSX Insecure Storage Mount

The Florida evaluation team found that the storage device within the AV-TSX platform was not implemented in the most secure manner possible. This vulnerability exposes the system to vote tampering attacks by malicious users.

The Assure 1.2 software release corrects this issue.

3.3.8 AV-TSX System Configuration Information is Unprotected

The Florida evaluation team found that a large portion of the system configuration for the AV-TSX platform is stored in the system registry. Alteration was found to be feasible by a malicious user.

The Assure 1.2 software release does not address this issue. Premier Election Solutions does not believe that a security risk is posed by this issue.

3.3.9 AV-TSX Ballot Definition File is Unprotected

The Florida evaluation team found that the ballot definition file uses an encryption method which is not considered to implement the highest level of security.

The Assure 1.2 software release addresses this issue by increasing the security of the ballot definition file protection using HMAC-SHA-1 (Hash Message Authentication Code Secure Hash Algorithm 1).

3.3.10 AV-TSX No Integrity Protection of Stored Electronic Ballots

The Florida evaluation team found that the encryption method used to secure the election database file was not implemented in the most secure manner possible. The Florida team made recommendations to Premier Election Solutions regarding security enhancements.

The Assure 1.2 software release addresses this issue by increasing the security of the stored electronic ballot file protection using HMAC-SHA-1 (Hash Message Authentication Code Secure Hash Algorithm 1).

3.3.11 AV-TSX Ballots are Stored Sequentially

The Florida evaluation team found that the ballots are stored within the AV-TSX system in the order in which they are cast. Users with encryption key access could potentially correlate voters to ballots and undermine the anonymity of the election.

The Assure 1.2 software release does not address this issue. Premier believes that in order to exploit this issue the malicious user would require access to the encryption keys within the AV-TSX system. The encryption keys are not externally accessible by the user and as such Premier believes that this issue does not represent a vulnerability.

3.3.12 AV-TSX Candidate Information is Not Stored in the Results File

The Florida evaluation team found that the candidate information on a ballot is not stored and a malicious user might use this vulnerability to tamper with vote counts.

The Assure 1.2 software release does not address this issue. Premier believes that this is not a security vulnerability.

3.3.13 AV-TSX Audit Logs Are Not Cryptographically Protected

The Florida evaluation team found the AV-TSX audit logs are protected in the same manner as the electronic ballots. Improved encryption methods exist and are outlined by the Florida team.

The Assure 1.2 software release addresses this issue by increasing the security of the AV-TSX audit log protection using HMAC-SHA-1 (Hash Message Authentication Code Secure Hash Algorithm 1).

3.3.14 AV-TSX Data is Neither Authenticated Nor Encrypted Over the Communication Link

The Florida evaluation team found that although SSL an available protocol within the system its use is optional. Further, the Florida team found issues with the Premier Election Solutions implementation of the SSL protocol.

The Assure 1.2 software release corrects this issue. Florida reviewers found that the implementation of the SSL protocol was not initialized with sufficient entropy to ensure secure communications. The Assure 1.2 software increases the entropy of the SSL protocol seed.

3.3.15 AV-TSX Bootloader Automatically Replaces Itself

The Florida evaluation team found that the bootloader process automatically replaced itself if a new copy of the bootloader file was found on the memory card. The Florida team made recommendations to improve the security of the bootloader replacement process.

The Assure 1.2 software release corrects this issue. Updating the bootloader software now requires both operator and bootloader software authentication.

3.3.16 AV-TSX Bootloader Automatically Replaces Operating System

The Florida evaluation team found that the AV-TSX bootloader could cause the operating system to be replaced if certain file types were found on the system memory card.

The Assure 1.2 software release corrects this issue. Updating the operating system now requires both operator and operating system software authentication.

3.3.17 AV-TSX Bootloader Automatically Runs .ins File on the Memory Card

The Florida evaluation team found that the AV-TSX bootloader automatically ran files with an extension of .ins. Although the .ins files on the memory card are signed the Florida team found the signatures to have vulnerabilities within the AV-TSX system.

The Assure 1.2 software release corrects this issue. The software now requires authentication of the user and of the .ins file proper to execution of .ins files.

3.3.18 AV-OS Leaks Memory Card Contents

The Florida evaluation team found that the contents of an AV-OS memory card could be obtained by interfacing a laptop computer to the AV-OS and using built-in Microsoft Operating System tools.

The Assure 1.2 software release does not address this issue. Premier Election Solutions believes that this vulnerability can be mitigated by the physical security measures of locking the AV-OS onto the ballot box and by locking the Yes / No keys on the AV-OS machine.

3.3.19 AV-OS Supervisor PIN Not Cryptographically Protected

The Florida evaluation team found that the supervisor access PIN was vulnerable to attack by a malicious user if the user was familiar with the method used to secure the supervisor access PIN.

The Assure 1.2 software release does not address this issue. Hardware limitations within the AV-OS platform do not allow for secure supervisor PIN storage. Premier Election Solutions recommends that users implement procedural security mitigations by strictly controlling supervisor card access.

3.3.20 AV-OS No Authentication Between GEMS and the Terminal

The Florida evaluation team found that no authentication exists on the communications channel between the AV-OS and the GEMS server.

The Assure 1.2 software release does not address this issue. Premier Election Solutions does not believe that this is a security vulnerability because the upload of data to the GEMS system is intended for the release of unofficial results only.

3.3.21 AV-OS Attacker Can Hide Pre-loaded Votes

The Florida evaluation team found that multiple different attacks existed in which the ballot count could be compromised. The attacks formulated were based on the previously identified weaknesses in the security key implementation and memory card integrity.

The Assure 1.2 software release corrects this issue. Details about how this issue was corrected were not provided by Premier Election Systems.

3.3.22 AV-OS Vote Counters Are Not Directly Checked for Overflow

The Florida evaluation team found that the vote counters associated with individual candidates were not checked for overflow and were thus subject to potentially insecure conditions. Not specific attacks were presented.

The Assure 1.2 software release corrects this issue. Details about how this issue was corrected were not provided by Premier Election Systems.

3.3.23 AccuBasic Interpreter Faults

The Florida evaluation team identified a number of different AccuBasic issues in their reports which either compromise or reduce system security. These issues are:

3.3.23.1 Error Checking is Inadequate

The Assure 1.2 software release does not address this issue. Premier Election Solutions does not believe that this is a vulnerability.

3.3.23.2 Error Codes Returned by the AV-OS System are Ignored

The Assure 1.2 software release does not address this issue. Premier Election Solutions does not believe that this is a vulnerability.

3.3.23.3 Unchecked String Operation: Allows Overwrite of Stack Memory

The Assure 1.2 software release corrects this issue. Premier Election Solutions did not provide details about how this vulnerability was addressed.

3.3.24 GEMS AccuBasic Scripts are Not Authenticated on the GEMS Server

The Florida evaluation team found that the GEMS server does no checks on the AccuBasic bytecode. All bytecode validation is performed from within the AV-OS and AV-TSX platforms using the encryption signatures. The Florida team previously found the signatures used to have vulnerabilities.

The Assure 1.2 software release does not address this issue. Premier Election Solutions believes that the authentication of the AccuBasic scripts on the AV-OS and AV-TSX platforms is sufficient to ensure security.

3.3.25 GEMS Password Does Not Protect Access to GEMS or Audit Logs

The Florida evaluation team found that using a simple, publicly known attack, access to the GEMS database and audit logs could be obtained from within the Windows Operating System.

The Assure 1.2 software release corrects this issue. Database access within the Assure 1.2 software release is password protected.

3.3.26 GEMS Incomplete Implementation of the SSL Protocol

The Florida evaluation team found that the use of the SSL protocol within the GEMS server is optional. The Florida team found then even when the SSL protocol was enabled security vulnerabilities still existed.

The Assure 1.2 software release does not address this issue. Premier Election Solutions believes that disabling the SSL protocol feature with the GEMS system is a security choice and advises customers to use the SSL features. Premier Election Solutions does not believe that their implementation of SSL is insufficient.

3.4 Other states using the Assure 1.2 platform

The Premier Election Solutions Assure 1.2 software release is currently certified for use in the state of Florida. Actual installation of the Assure 1.2 platform had not yet occurred at the time that this report was written.

All other customers of Premier Election Solutions require the same VSS certification as the State of Alaska in order to implement Assure 1.2. As such Assure 1.2 has not been installed on any known systems in the United States.

No known AccuVote systems have used the Assure 1.2 revision in a live election.

3.5 Division of Elections AccuVote Security Enhancements and Features Evaluation

The State of Alaska Division of Elections provided the UAA project team with a list of suggested security improvements during Phase 1. This list of enhancements and features is provided in "Appendix L – State of Alaska, Division of Elections Accu-Vote Security Enhancements and Features".

This section evaluates the DoE enhancements and features against the Assure 1.2 software revision enhancements. Cases where the issue identified by the DoE are resolved or mitigated by the Assure 1.2 software or firmware are presented in this section.

3.6.1 Verify GEMS Certified Software Has Not Been Altered

The Division of Elections desires to compute a hash code of the GEMS software to ensure that the currently running version has not been compromised.

The Assure 1.2 software release addresses this issue. Premier Election Solutions Premier's Windows Configuration Guide, Revision 3.0, Section 10 (2007) provides a detailed procedure for hash code validation of the GEMS software.

3.6.2 AV-OS / AV-TSX Supervisor Mode Password Changes

The Division of Elections desires to change the supervisor access passwords for the AV-OS and AV-TSX devices as regular intervals.

The Assure 1.2 platform in combination with the Keycard Tool application allows authorized users to change the supervisor access password for the AV-TSX device. The Assure 1.2 platform allows the authorized users to change the supervisor PIN for the AV-OS device.

3.6.3 AV-OS / AV-TSX Memory Card Wipe

The Division of Election desires to clear the memory of previous elections from all system memory cards prior to conduction of a new election.

The Assure 1.2 software release does not address this issue. Premier Election Solutions recommends using the AV-OS diagnostic menu to erase the contents of the AV-OS memory card. An external PCMCIA reader / writer is recommended for re-formatting the AV-TSX memory card units.

3.6.4 AV-TSX VVPAT Bar Code Removal

The Division of Elections desires to remove the time stamp bar code from the VVPAT printout.

The current software platform supports this feature.

4 Recommendations

It is the recommendation of the SOAESP project team that the State of Alaska, Division of Elections install the Assure 1.2 revision. Installation of this system revision is recommended for implementation following the 2008 election cycle.

Although the Assure 1.2 revision represents significant enhancements to system security two issues exist which make the installation of the Assure 1.2 revision impossible for the 2008 election cycle. Firstly, the Assure 1.2 revision software is not yet certified to the Voting System Standards (VSS) 2002 specification. The Assure 1.2 revision is currently in review with the nationally recognized testing agency SysTest. Formal certification from this agency has not yet been received by Premier Election Solutions and is required by Alaska State Law for installation on Division of Elections hardware. Secondly, the Division of Elections resources for the 2008 election cycle are not sufficient to complete the upgrade prior to the primary election which takes place in August, 2008.

It is recommended that the Assure 1.2 revision be implemented by the Division of Elections following the general election in 2008 and is contingent upon Premier Election Solutions receiving formal certification from SysTest.

Appendix C - Assure 1.2 Upgrade Issue Resolution Matrix

SOAESP Issue Number	Reference Document	Reference Document Section	Issue Description	Assure 1.2 Status
3.2.1	California Red Team Review	Section 3	Precinct Count AV-OS Ballot Tampering	Corrected by adding counter integrity checking with public counter
3.2.2	California Red Team Review	Section 4b	AV-TSX Malware	Corrected bootloader issue, Premier rejects format string error vulnerability
3.2.3	California Red Team Review	Section 4c	AV-TSX Escalation of Privileges	Corrected - can still enter system setup/diagnostics when peripheral device fails but cannot access administrative functions.
3.2.4	California Red Team Review	Section 4d	AV-TSX Default Static Key	No change, Premier believes default key indication is a feature.
3.2.5	California Red Team Review	Section 1b	GEMS Databases	Corrected - improved database security, corruption of database file (as compared to modification) by system administrator cannot be prevented since, by definition, the system administrator has full system access.
3.2.6	California Red Team Review	Section 1c	GEMS Audit Logs	The database is password protected in Assure 1.2. However, standard security practices with the GEMS server are critical.
3.3.1	Florida Analysis	Section 3.5	RSA signature flaw.	Corrected in Assure 1.2
3.3.2	Florida Analysis	Section 3.6	AV-OS Memory Card Integrity Is Not Protected	Complete authentication is beyond the capability of the AVOS hardware. While some improvements have been made, for example protecting the Abasic report scripts, physical protection of the memory card contains to play a critical role.
3.3.3	Florida Analysis	Section 3.7.1.1	AV-TSX Cryptographic Key Management	Premier recommends that all AV-TSX systems utilize the Keycard Tool Application
3.3.4	Florida Analysis	Section 3.7.1.2	AV-TSX Memory Card Update File is Unprotected	Corrected
3.3.5	Florida Analysis	Section 3.7.1.3	AV-TSX Smart Card Authentication Uses Only a Hard Coded Password	No change. The smart card does not use hard coded passwords. The issue was the authentication method used by the smart cards. This is mitigated procedurally by poll workers' monitoring for suspicious activity with smart cards or voters spending excessive time at the machine
3.3.6	Florida Analysis	Section 3.7.1.4	AV-TSX Supervisor PIN is Not Cryptographically Protected	No change. The issue is that the reviewer did not consider the protection robust enough rather than there not being any protected. Mitigated procedurally by restricting access to supervisor cards.
3.3.7	Florida Analysis	Section 3.7.1.5	AV-TSX Insecure Storage Mount	Corrected
3.3.8	Florida Analysis	Section 3.7.1.6	AV-TSX System Configuration is Unprotected	No Change - this is not a vulnerability since there is no ability to externally access this data.
3.3.9	Florida Analysis	Section 3.7.1.8	AV-TSX Ballot Definition File is Unprotected	Corrected - The file was actually protected but the reviewer considered the protection to be too weak. Have changed to using a SHA1 HMAC
3.3.10	Florida Analysis	Section 3.7.1.10	AV-TSX No Integrity Protection of Stored Electronic Ballots	Corrected - The file was actually protected but the reviewer considered the protection to be too weak. Have changed to using a SHA1 HMAC
3.3.11	Florida Analysis	Section 3.7.1.11	AV-TSX Ballots are Stored Sequentially	Exploiting this requires access to encryption keys of which there is no external ability to access.
3.3.12	Florida Analysis	Section 3.7.1.12	AV-TSX Candidate Information is Not Stored in the Results File	Premier disagrees that this is a security problem. No change
3.3.13	Florida Analysis	Section 3.7.1.13	AV-TSX Audit Logs Are Not Cryptographically Protected	Corrected - The file was actually protected but the FS review considered the protection to be too weak. Have changed to using a SHA1 HMAC
3.3.14	Florida Analysis	Section 3.7.1.14	AV-TSX Data is Neither Authenticated Nor Encrypted Over the Communication Link	Corrected - The issue was not that the data was not encrypted but that the seed used to initialize the encryption system did not contain enough entropy.
3.3.15	Florida Analysis	Section 3.7.2.1	AV-TSX Bootloader Automatically Replaces Itself	Corrected - Updating the bootloader now requires authentication of the operator and the new bootloader.
3.3.16	Florida Analysis	Section 3.7.2.2	AV-TSX Bootloader Automatically Replaces Operating System	Corrected - Updating the Operating System now requires authentication of the operator and the new Operating System
3.3.17	Florida Analysis	Section 3.7.2.3	AV-TSX Bootloader Automatically Runs .ins Files on the Memory Card	Corrected - Running an .INS file now requires authentication of the operator and the .INS file.
3.3.18	Florida Analysis	Section 3.8.1.1	AV-OS Leaks Memory Card Contents	Access to this capability is limited by locking the AVOS onto the ballot box and by locking the cover to the yes/no keys.
3.3.19	Florida Analysis	Section 3.8.1.2	AV-OS Supervisor PIN Not Cryptographically Protected	Due to hardware limitations, there is no secure storage for the PIN. Thus procedural mitigation is required, as it has been in the past.
3.3.20	Florida Analysis	Section 3.8.1.3	AV-OS No Authentication Between GEMS and the Terminal	This upload is for unofficial results only. The upload at election central occurs in a secure environment.
3.3.21	Florida Analysis	Section 3.8.1.4	AV-OS Attacker Can Hide Pre-loaded Votes	Corrrected
3.3.22	Florida Analysis	Section 3.8.1.5	AV-OS Vote Counters Are Not Directly Checked for Overflow	Corrected
3.3.23.1	Florida Analysis	Section 3.9.1	Error Checking Is Inadequate in AccuBasic	No Change The report failed to demonstrate any security risk.
3.3.23.2	Florida Analysis	Section 3.9.2	Error Codes Returned by the AV-OS System are Ignored	No Change The report failed to demonstrate any security risk.
3.3.23.3	Florida Analysis	Section 3.9.5	AccuBasic Unchecked String Operation	Corrected
3.3.24	Florida Analysis	Section 3.10.1	GEMS AccuBasic Scripts are Not Authenticated On the GEMS Server	No change. The scripts are authenticated on the AV-OS and AV TSx, not on the GEMS server
3.3.25	Florida Analysis	Section 3.10.2	GEMS Password Does Not Protect Access to GEMS or Audit Logs	The database is password protected in Assure 1.2

3.3.26	Florida Analysis	Section 3.10.3	GEMS Incomplete Implementation of the SSL Protocol	Disabling this feature is optional. Policy should be to enable this feature.
3.6.1	State of Alaska Division of Elections	GEMS Item 1	Verify GEMS Certified Software Has Not Been Altered	Hash code validation procedures for software installed on GEMS servers are documented in section 10 of *Premier's Windows Configuration Guide Rev 3.0*.
3.6.2	State of Alaska Division of Elections	Memory Card Item 6	AV-OS / AV-TSX Supervisor Mode Password Changes	Use of the Keycard Tool application allows password changes on AV-TSX. Authorized Users may change the Supervisor PIN on the AV-OS platform
3.6.3	State of Alaska Division of Elections	Memory Card Item 9	AV-OS / AV-TSX Memory Card Wipe	While Premier does not offer a wipe utility *per se*, AVOS memory cards may be erased in diagnostic mode on the AVOS. TSx memory cards may be reformatted in a non-network-connected, known secure computer with a PCMCIA card reader.
3.6.4	State of Alaska Division of Elections	Voting Equipment Item 2	AV-TSX VVPAT Bar Code Removal	System is capable of bar code removal

Appendix D - Division of Elections Enhancement Analysis

1. Introduction

This document evaluates the State of Alaska, Division of Elections AccuVote Security Enhancements and Features (2007) document to determine whether the proposed changes to the system are feasible in the currently implemented system.

Each suggested enhancement or feature listed in this document is presented as shown in the State of Alaska, Division of Elections AccuVote Security Enhancements and Features (2007) document and is followed by a discussion and recommendation regarding that enhancement or feature.

2. Enhancement / Feature List

2.1 Software Hash Validation

Description

Verify the certified software installed has not been altered by computing the digital signatures of the software and comparing them with the digital signatures of the certified version.

The digital signature comparison should be performed at least:

a. Immediately after installing a new component or new version of software.
b. After any unusual or suspicious event.
c. Before beginning the set-up of a new election.
d. Immediately after completing an election.

Comments / Recommendation

Calculation of the digital software signature for the components operating on the GEMS server and on personal computer based software components or applications (Key Card Tool, VC Programmer) is recommended. The suggested hash validation plan presented by the Division of Elections is reasonable. Although hash validation of the EPROM chips present in the AV-OS machines is possible the logistics associated with removal and validation of the EPROM chips prior to each election cycle is significant. As such we recommend validating hash codes on AV-OS machines only on an individual case by case basis in circumstances where an unusual or suspicious event has occurred. We also recommend the use of tamper evident markers on the EPROM chips as well as marking each EPROM chip with a unique serial number to increase the confidence in the AV-OS firmware and lessen the requirement for periodic hash code validation of the AV-OS firmware.

2.2 GEMS Network Access and Exclusive Use

Description

Ensure that no GEMS computer is connected to a network or the internet and do not allow any software on the GEMS computer except for the voting system software itself. Use only the GEMS computer for programming an election.

Comments / Recommendation

It is crucial to the security of the GEMS servers that local network and internet connectivity be avoided. As such careful attention must be paid not only to ensuring that connectivity does not exist but also to ensuring that connectivity would be difficult or impossible to achieve by malicious users. The GEMS server should not be housed in close proximity to other network access equipment including packet communications switches, routers, etc. Premier Election Solutions Premier's Windows Configuration Guide (2007) provides detailed configuration information regarding the acceptable configuration of GEMS servers to be used in an AccuVote system. It is recommended that the Division of Elections follow these guidelines. The GEMS server should be exclusively used for the purpose of programming elections and for no other purpose (specifically it is recommended that any implementation of the Key Card Tool application be performed on a separate personal computer platform dedicated to that purpose).

2.3 Authorized GEMS Access Restriction

Description

Restrict access to the voting system to authorized personnel only and maintain an access log to record each time a person accesses the GEMS computers.

Comments / Recommendation

Maintaining a secure system by limiting access only to authorized personnel is recommended. Authorization to obtain access to the GEMS system should be based on individuals completing security training. This security training should familiarize the user with standard security procedures for use with personal computers, the Windows operating system and the GEMS software specifically. The use of access logs is not a recommended enhancement given the small number of system users (see "Appendix E – Physical Password Management Recommendations", Section 2 Recommendation 2).

2.4 Election Program Control

Description

Do not allow any changes to the election program once the logic and accuracy testing has commenced.

Comments / Recommendation

Knowledge of the election program status at all times in the election process is recommended. The Division of Elections current implementation of locking the election program once logic and accuracy testing has begun is recommended to ensure consistency and validity of the test results.

2.5 Voting System Access Control

Description

Never allow vendor personnel to access the voting system unless an authorized member of election staff is present.

Comments / Recommendation

Supervision of all non-staff individuals requiring access to the election system is recommended. Vendor supervision is strongly recommended.

2.6 Password Management Policy

Description

Establish policy for password management. Change passwords on a periodic basis and at least once an election cycle or once a year.

Comments / Recommendation

Management of the passwords utilized with the Division of Elections AccuVote system is crucial to implementing a secure, reliable election system. We recommend following the password management guidelines presented in the attached "Appendix E - Physical Security and Password Management Recommendations". This document outlines a password management strategy which incorporates the challenges faced by election officials working in the State of Alaska.

2.7 Background Checks

Description

Perform background checks on staff authorized to:

a. Define and configure elections
b. Maintain voting equipment
c. Enter election results into GEMS
d. Gain access to voting system or system components

Comments / Recommendation

We recommend requiring background checks on new employees (authorized to perform tasks list above) in accordance with state and labor union regulations.

2.8 Director's Office Memory Card Storage

Description

Memory cards stored in the director's office are to be maintained in a secured environment.

Comments / Recommendation

Secure storage of the AccuVote memory cards is strongly recommended. Physical access security precautions outlined in "Appendix E - Physical Security and Password Management Recommendations" are recommended to be used for secure all election components deemed vulnerable to malicious attack.

2.9 Memory Card Chain of Custody

Description

Memory cards, once programmed and tested, that are shipped to the regional offices need to be shipped using chain-of-custody security measures.

Comments / Recommendation
We recommend using a shipper (such as DHL, FedEx, Alaska Airlines Gold Streak) with chain of custody processes to transport memory cards to regional offices prior to elections.

2.10Regional Office Memory Card Storage

Description

Once memory cards are received in regional offices they are to be maintained in a secured environment.

Comments / Recommendation

Secure storage of the AccuVote memory cards is strongly recommended. Physical access security precautions outlined in "Appendix E - Physical Security and Password Management Recommendations" are recommended to be used for secure all election components deemed vulnerable to malicious attack.

2.11Memory Card Tracking Audit Capability

Description

Have audit / receipt tracking form to compare against sent memory cards and received memory cards that is signed off.

Comments / Recommendation

The ability to track and account for all memory cards system-wide is highly recommended. We recommend implementing a bar-code inventory process next year (after elections) and including memory cards in the inventory.

2.12Memory Card Pre-election Tamper Security

Description

Send memory cards to election board in tamper-sealed envelopes for insertion into the units on election morning. Require election board to verify envelope is sealed prior to opening and sealing memory card in voting unit. Since equipment is in the possession of the election chairperson prior to election day, keeping the memory cards sealed until election morning removes the possibility of tampering with the memory card by the person with possession.

Comments / Recommendation
We agree that that Division should ship memory cards in tamper evident envelopes and that the election board verifies the integrity of the seals and insertion of the cards into machines (if the memory card hasn't already been installed in the voting machine).

2.13Supervisor Mode Password Change

Description

Consider password changes to access supervisor mode.

Comments / Recommendation

It is highly recommended that the password utilized to access supervisor mode be changed at a minimum once per election cycle and that the distribution of the supervisor password be strictly limited to election officials requiring supervisor access only.

2.14Memory Card Inventory Accounting

Description

Maintain inventory log and accountability of all memory cards with election programming to ensure all cards are returned after the election.

Comments / Recommendation

It is recommended that the measures recommended in section 2.11 be used to confirm the receipt of all returned memory cards used during an election cycle.

2.15Battery Replacement Schedule

Description

Establish a timeline for battery replacement of memory cards.

Comments / Recommendation

Premier Election Systems documentation specifies memory card battery life at 5 years. It is recommended that the Division of Election replace AV-OS memory card batteries every other election cycle or when the memory card battery life indicator shows a low battery. Documentation of the battery replacement plan should be developed to ensure that historical battery replacement chronology can be produced as need.

2.16Previous Election Memory Card Wipe

Description

Establish a timeline of previous elections information to be removed from memory cards.

Comments / Recommendation

It is recommended that the contents of each memory card be cleared prior to each election (primary and general).

2.17AV-TSX VVPAT Flap Removal

Description

Remove the flap from the VVPAT viewing location so voters know they can review the paper version of their ballot.

Comments / Recommendation

It is recommended that the VVPAT flap on the AV-TSX machine be modified to include a label which instructs the voter to lift the VVPAT flap to review the voted ballot. This implementation retains voter privacy while ensuring that the voter is aware of the ballot review feature.

2.18AV-TSX Bar Code Removal

Description

Remove the bar code from the VVPAT ballot.

Comments / Recommendation

It is recommended that the bar code printed on the AV-TSX VVPAT ballot be deactivated in the BallotStation software to lessen the probability of voter identification after using the AV-TSX machine and increase voter anonymity.

2.19AV-TSX Use Encouragement

Description

Encourage at least 5 votes cast on the touch screen as a means of protecting voter privacy with the use of the reel-to-reel printer.

Comments / Recommendation

It is recommended that precinct officials encourage voters to use the AV-TSX machines as much as possible to reduce the risk of voter privacy violations. A minimum of 5 votes should be considered the absolute minimum vote count required for the AV-TSX and more votes should be encouraged.

2.20 Voting Machine Tracking and Accounting

Description

Maintain record of the serial number of each voting unit and which precinct the unit was sent to.

Comments / Recommendation

It is recommended that the serial number, firmware / software versions and functional test results from each election cycle along with the destination precinct be recorded and maintained in electronic historical archives.

2.21 Physical Security Review

Description

Conduct a physical security review to assess the access and control procedures for areas where voting equipment and components are stored and maintained. Establish policy for access to area where equipment is stored, including the restriction of vendor and non-election employees to have uncontrolled access.

Comments / Recommendation

We recommend that the physical security recommendations outlined in "Appendix E – Physical Password Management Recommendations" be implemented in the 2008 election cycle. We further recommend that the Division of Elections conduct a physical security review using a professional security agency at each location where voting equipment is stored.

2.22 Asset Management Plan

Description

Implement asset management and inventory control system for voting equipment and components, including the software and firmware installed on each piece of voting equipment.

Comments / Recommendation

It is recommended that the functional testing, voting machine tracking and accounting (section 2.20) and the asset management plans be incorporated into a single procedure in which a complete documentation package is produced for each voting machine during each election cycle. The contents of the documentation package should be scanned into electronic format for long term archival storage.

2.23 Tamper Evident Seals

Description

Implement the use of tamper-evident seals.

Comments / Recommendation

We recommend that the Division of Elections use tamper-evident seals on AV-OS and AV-TSX machines. Section 1.6 of the main document includes a detailed description of this recommendation

2.24Vendor Repair Acceptance Testing

Description

Implement testing procedures and sign-off on all equipment returned from vendor after maintenance and / or repair to ensure proper versions of the hardware, software and firmware.

Comments / Recommendation

It is recommended that acceptance testing and documentation be performed prior to accepting equipment returned from the vendor for repair or maintenance. The acceptance test procedure should follow the tests outlined in "Appendix M - AccuVote Functional Test Guidelines". Documentation confirming that the returned machine passed the required tests should be produced and stored electronically in the historical archive.

2.25AV-TSX Inter-election Storage

Description

Consider process for the storage of touch screen voting units in remote areas of the state between the Primary and General elections.

Comments / Recommendation

We recommend storing touch screen voting units in locked closets or cabinets between elections. However, the machines take up a lot of space, and this may not be possible. In which case we recommend storing them in a lockable facility.

2.26Functional Test Guidelines

Description

Establish functionality testing schedule and procedures for all voting equipment.

Comments / Recommendation

It is recommended that the Division of Elections adopt the functional test guidelines presented in "Appendix M - AccuVote Functional Test Guidelines". This document outlines a suite of tests and provides recommended documentation guidelines for use with the AccuVote system in the State of Alaska.

2.27Logic and Accuracy Test Improvements

Description

Update logic and accuracy testing reports for voting equipment based on where equipment is used, polling places, early voting ballot counting at regional offices.

Comments / Recommendation

It is recommended that the Division of Elections adopt the logic and accuracy improvements and enhancements outlined in “Appendix N - AccuVote Logic and Accuracy Test Guidelines”. This document details a suite of logic and accuracy tests and documentation guidelines to help ensure tabulation accuracy and election programming validity.

2.28Post Election Audit Validation

Description

In post-election audit, compare all election results transmitted via modem from the polling place against the actual results printed by the election board prior to transmission.

Comments / Recommendation

It is recommended that the transmitted results be compared with the printed results to confirm accuracy. Inconsistencies between the transmitted results and the printed results must be documented and resolved prior to official results being released by the Division of Elections.

2.29Central Administrator Card Controls

Description

Establish inventory controls and procedures for the security of the Central Administrator Cards for touch screen voting system.

Comments / Recommendation

It is recommended that the AV-TSX Central Administrator cards be secured in the highest security area and passwords associated with the Central Administrator card be given only to authorized individuals requiring Central Administrator access.

2.30Security Standards for Loaned Voting Machines

Description

Establish basic security standards of voting equipment that is used or stored by city / borough entities.

Comments / Recommendation

It is recommended that entities utilizing State of Alaska owned voting machines should be trained regarding election system security and the policies adopted by the State of Alaska. Complete functional testing of loaned voting machines should be performed upon return of the voting machines to the Division of Elections. Documentation of these tests should be produced and archived.

2.31Municipal Owned Machine Use Policy Review

Description

Consider policy on the use of municipal owned voting equipment being used in state and federal elections. There is a location in the state where the municipality owns the optical scan and the state uses it during elections.

Comments / Recommendation

It is recommended that the State of Alaska procure enough machines to service all precincts required and that the State of Alaska not utilize machines owned and stored by other government entities.

Appendix E - Physical Security and Password Management Recommendations for GEMS Servers

1. System Overview

This document describes the existing safeguards employed by the State of Alaska, Division of Elections to protect the Global Election Management System (GEMS) hub and regional servers. The discussion is limited to the physical security and the password mechanisms in place that relate to the GEMS servers. Related topics, such as recommended Windows configurations, disaster planning, or malware prevention are not discussed here.

The security mechanisms consist of the physical building security and three layers of password-protected systems: BIOS (Built-In Operating System) password, Windows authentication, and GEMS Database server authentication. These mechanisms are depicted in Figure 1.

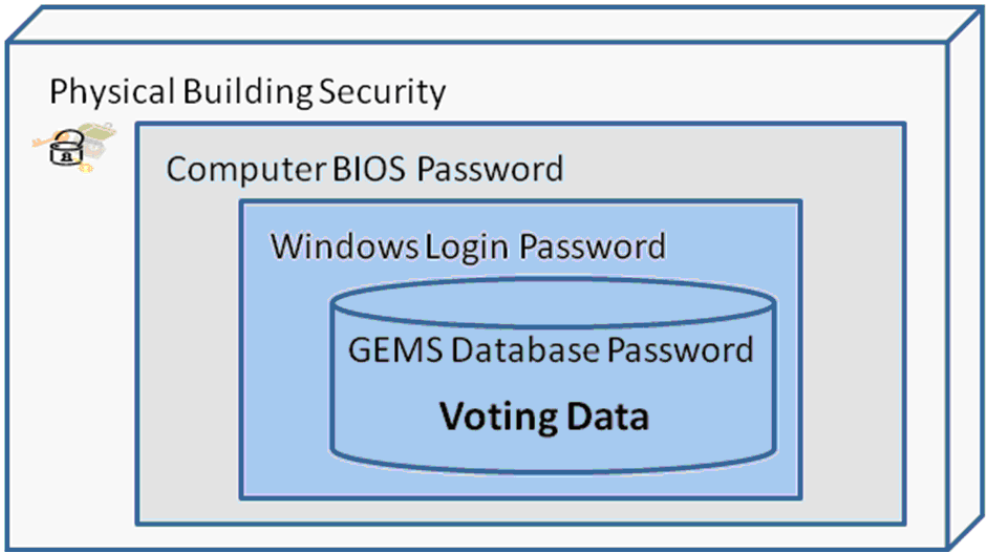


Figure 1. Layers of protection afforded by passwords and physical security

1.1 Existing Physical Security

The Division of Elections maintains eight GEMS servers, two host servers for Director's Office use (one is a backup), one for Region I (handcount use), one for Region II (handcount use), two for Region III (multiple servers for handcount efficiency), two in Region IV (multiple servers for handcount efficiency). The host server is used to program the databases for dissemination to the regional GEMS server prior to an election and for aggregating results from the regional GEMS servers after an election. Several regional supervisors reported that the regional GEMS servers are not frequently used – they are primarily used to hand-enter election results from hand-count precincts and for hand-count results entry in precincts where the AV-OS upload has failed.

The host server is administered by the GEMS programmer. The GEMS programmer also sets accounts and passwords for the regional servers that are operated by the regional Election Supervisors. The physical security varies by location, but it is the Division of Election's policy to keep all GEMS servers, voting equipment, and components of the voting systems (e.g. memory cards) in a locked and/or alarmed room.

- Host server: Juneau

  The host server is located in a locked, alarmed room. Three employees have access to the room. The door is unlocked by a key that is stored in a private desk drawer.

- Region I: Southeast

  The GEMS server is located in a locked, alarmed room. The election equipment is located in a separate locked room that can be alarmed. Two employees have access to the rooms.

- Region II: Anchorage and Matanuska Valley

  The GEMS server is located in a locked, alarmed room together with the touch screen units. The optical scan units are stored in an outer room, also locked and alarmed. Three employees have access to the GEMS server room. An additional key is available to staff, but only the three employees know the alarm access code.

- Region III: Fairbanks and Interior

  The GEMS server is located in a locked room. Three employees have access to the server room. Unlike the other regions, activity in this room is high since a staff member has a desk located in the room.

- Region IV: Nome, Barrow and West Coast

  The GEMS server is located in a locked back conference room. Two employees have access to the room which also stores other election equipment.

Access to the rooms is limited to authorized Division of Elections employees. All non-employees entering the room must be accompanied by an authorized Division of Elections employee. Division employees go in and out of the rooms frequently and do not maintain an entry or exit log.

1.2 Existing Password Management Policies

Systems that may be secured by password include alarm access codes, BIOS passwords, Windows login passwords, and GEMS database passwords.

Alarm access codes consist of a numeric PIN and are used to enable or disable the alarm system, if one exists.

A BIOS password requires the user to enter a password to boot the system. This may be enabled in the BIOS for the GEMS servers. Only a single password is stored; i.e. there is

no per-user authentication. The password is stored in flash memory or refreshed by an internal battery. None of the Division of Elections supervisors reported that a BIOS password was enabled on their server.

Windows login passwords are used to log into the GEMS servers, which are currently running a version of Windows 2000. There is only one account for each server and users share accounts. For example, there is a generic user account used by two different users to log in for a given GEMS server. The number of users sharing an account is never more than three and is typically a single user. Regional supervisors were unsure about details of account policies, including password aging (a mandatory change to a new password after some time period has elapsed), number of re-tries if an invalid password is entered, and password generation details. The regional supervisors indicated that the account policies should be identical to the host server, which reportedly locks out users after three failed attempts and implements password changes every election cycle. However, one regional administrator reported that the Windows password had not been changed, indicating that mandatory password aging has not been implemented in all cases.

The GEMS database stored on each GEMS server is further protected by a database-level password. Prior to every election the GEMS host programmer sends the election database to the regional supervisors. The database is sent physically on a CD and shipped via a tracked shipping method. Access to the database requires a username and password which is set in the master database at the time of creation. The username and password are changed once every election cycle. The usernames and passwords are selected and discussed during the senior manager's conference call and typically consists of a phrase with mixed case letters and numeric characters. The usernames and passwords are shared with the regional supervisors via telephone call. The process is illustrated in Figure 2.

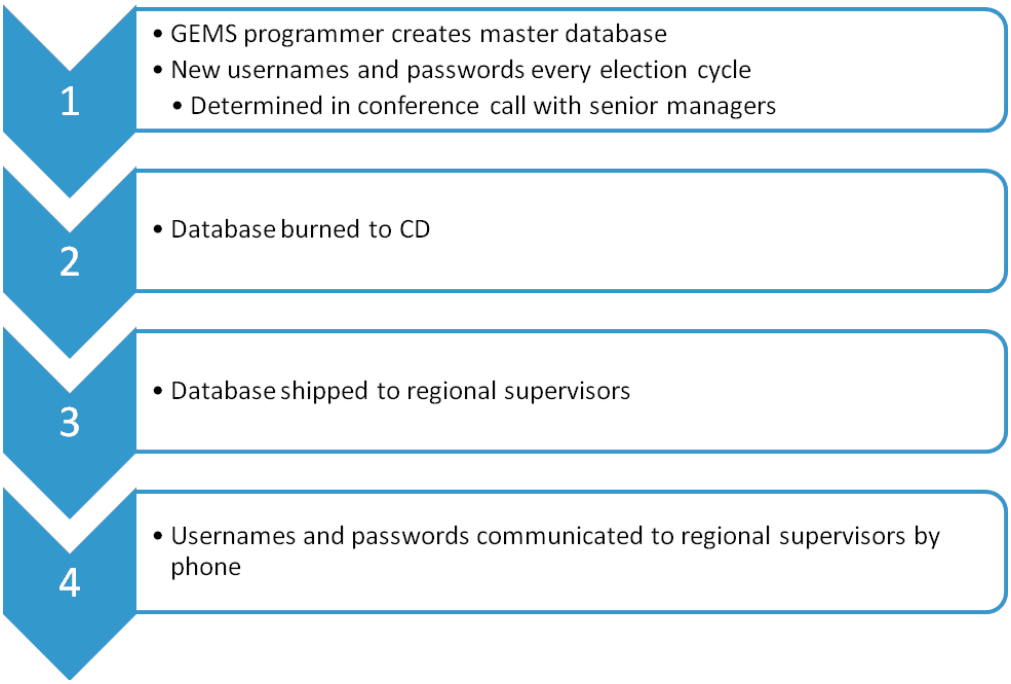


Figure 2. Distribution mechanism for GEMS database usernames and passwords

At the time of this report, there are seven usernames and passwords. The database username and password is always different from the Windows login username and

password, although in most cases when a user logs in on the same regional GEMS server they will use the same Windows login and the same database login.

2. Physical Security Recommendations

In the GEMS system, physical security arguably presents the greatest opportunity to deter malicious attack. Given unfettered access and sufficient time a determined attacker will likely be able to circumvent the BIOS, Windows, and database passwords. Removing physical (and remote) access eliminates many avenues of attack.

Our recommendations for physical security are similar to many of Premier's recommendations described in the Client Security Policy documentation (Diebold Election Systems, 2007) but have been adjusted for the Division of Elections work environment.

Our recommendations are to:

1. Fortify the structure enclosing the GEMS server and associated infrastructure so it may not easily be entered by force.

2. Do not maintain entry and exit logs to the GEMS server rooms. This is not practical given the high volume of access in several locations, primarily by the same employees. We recommend continuing the practice of requiring an authorized Division employee to be in the room at all times to supervise any non-authorized persons are in the room.

3. At a minimum, continue to secure the GEMS server and associated infrastructure in a locked room. We also strongly recommend a monitored alarm system. Other considerations include a video surveillance system, fireproof door, temperature controls to maintain the temperature between 50-80 degrees Fahrenheit, and a two-factor entry system. Two-factor authentication requires two methods to enter the room (e.g. key and biometric fingerprint scanner, key and alarm passcode, etc.)

4. Where feasible the GEMS server and associated infrastructure should NOT be stored in the same room as other election equipment (e.g. touch screen or optical scan units) to physically separate those personnel authorized to access the other election equipment but not the GEMS server.

   In instances where it is not feasible to physically separate the GEMS server from other election equipment the equipment storage area should be used exclusively for storage. All testing, tabulation, validation and other process related activities should be performed in a workspace separate from the GEMS storage area. Access to the GEMS servers should be carefully monitoring and limited to authorized personnel only.

5. All doors should be locked when the equipment is not in use.

6. Practice the principle of least access. Access to the GEMS server room should be kept to the minimum number of privileged personnel.

7. Establish a procedure to regularly inspect and maintain physical locks and test alarm systems.

8. Keys to the GEMS server room should not be left in a location accessible to non-authorized personnel (such as cabinets or drawers). Authorized personnel should carry a key on their person or store it in a securely locked location, such as a safe. Any non-authorized personnel wishing to enter the room must have an authorized employee open the door and monitor the non-authorized personnel's activity while in the room.

9. The server should have a locked bezel to deter disk bays from being accessed or the cover from being opened.

10. Establish a written, formal physical security policy that addresses the above considerations and includes policies to change access codes or keys when employees leave, backup and recovery procedures, backup power, fire emergency plan, and procedures to periodically review existing or new physical security controls. These procedures should assess known risks and identify vulnerabilities associated with the physical environment. This periodic review is necessary because appropriate policies and procedures may need revision as technology changes over time, or vice versa.

3. Password Management Recommendations

Passwords provide a secondary line of defense if physical security is compromised. We recommend employing BIOS passwords as an additional security control on top of the Windows and GEMS database passwords. All passwords should be "strong" in the sense that they are not easily guessed or determined through systematic means.

An example of a weak password is any word found in a dictionary. An attacker could determine the password by brute force, trying every word in the dictionary (automated by a program) until the password is found. Another weak password is one that is too short or selected from a small set of characters. Consider a 4-character password comprised of lowercase letters. This allows $(26)^4$ or 456,976 possible passwords. A brute force program could easily enumerate all possibilities and quickly determine the password. However, if the set of characters is expanded to include uppercase letters and digits, and the length is increased to 8, then the number of passwords becomes $(62)^8$ or 2.2×10^{14}, a much larger number that makes the password more difficult to guess or determine through brute force.

However, we must recognize that strong passwords alone do not guarantee protection. For example, an attacker could bypass the Windows login password by physically removing the hard drive and mounting it on a separate system to examine its contents. Similarly, the strongest passwords are useless if an unauthorized observer "shoulder surfs" by watching the keys pressed by an authorized user as she enters her password, or if the passwords are discovered by an attacker on a written piece of paper. Moreover, in the case of the GEMS servers, the security of the underlying operating system is much easier to break than the password security. As one example, the RABA report (RABA Technologies LLC, January 20, 2004) describes how to exploit a Windows bug on an unpatched GEMS server to gain administrator access by merely dialing into the system's modem with a software product called Canvas. Additional defensive controls must be in place to secure the system and the passwords themselves to mitigate potential attack.

3.1 Tradeoffs between usability and password strength

While longer and more complex passwords increase the cryptographic strength, a tradeoff must be made with usability, i.e. the ease of which users are able to work with the system. For example:

- Long and complex passwords are hard to remember.
- If a password is hard to remember then it is more likely to be written down, providing an attacker easy access if the written password is discovered.
- If a user has to remember many passwords then it is more likely they will be written down, providing an attacker easy access if the written passwords are discovered.

A balance must be made between password length, number, and memorability. We recommend the following criteria for password selection and storage:

1. Passwords should be at least 8 characters and include mixed-case, at least one digit, and at least one non-alphanumeric character.
2. Ideally, passwords should not be written down or the risk of disclosure will increase. If they must be written down then the password must be stored in a secure, non-obvious location that is not in the same room as the server. For example, we do not recommend storing the password in a desk (even if locked) in the server room or in the desk of the employee that commonly frequents or manages the server room. A safe would constitute a secure location.
3. Optionally, to increase the memorability of passwords, several techniques are possible, such as concatenating the first few letters of words in a phrase while inserting digits or non-alphanumeric characters. For example, if the phrase is "**sec**ure **ele**ctions **eve**ry **tim**e" then the password could be **sec**4**ele**+**eve**&**Tim**. Recent research indicates that using such mnemonic passwords schemes still leaves the system vulnerable to smart-dictionary types of attacks (Kuo, Romanosky, & Cranor, 2006), although the vulnerability is likely to be exploited only in the more distant future
4. The same password should never be used in a different system. For example, the BIOS password should not match the GEMS password. Similarly, the Windows password should not match an employee's personal Google password.

A related and sometimes contentious issue is password aging, or the practice of forcing users to change their passwords after a certain number of days has elapsed. A password history can also be kept so users cannot revert to a previous password.

The major benefit of password aging is to safeguard against guessing and unknown disclosure. For example, if a password has not been changed for years but has been leaked unbeknownst to the owner, perhaps through accidental disclosure, then regular password changes will prevent an unauthorized user from logging in. We include "unbeknownst to the owner" because if the leak is known then the password should be changed immediately and the machine examined for tampering.

Conventional wisdom and the Diebold Client Security Policy (Diebold Election Systems, January 11, 2007) suggest a password age no more than 45 days and a history of 10 passwords. However, the benefits of password aging are fairly modest and can actually be destructive (Spafford, 2006):

- Password changes offer no protection against password snooping and operating system level attacks.

- Frequent password changes make the password harder to remember and becomes more likely to be written down, increasing the potential for disclosure.

- To generate a new and memorable password that is not in the history list, many users use an algorithm that can be easily guessed, such as appending a different digit onto the end of the password. This practice also increases the potential for guessing if old passwords are disclosed.

- If a password has been obtained by an attacker then the mandatory password change is likely weeks away, giving the attacker many days to authenticate and attack the system. This scenario can be mitigated by incorporating additional security controls that the attacker must also confront. For example, if an attacker discovers the password but doesn't yet have a way to get into the room then password aging will thwart the attacker if the password is changed before the attacker finds a way to gain physical access.

Due to the relatively modest gains of password aging and the negative impact on memorability we suggest a less aggressive aging schedule than the Diebold recommendations. Specific recommendations relating to password aging are given in the following sections. Our recommendations regarding password management have also been targeted specifically for the Alaska Division of Elections GEMS environment. For example, with less than 10 users and infrequently used servers, the same policies are not always appropriate that would be used in the common IT scenario involved in authenticating hundreds of users on an enterprise network.

3.2 BIOS Password

A BIOS password prevents the system from booting if an incorrect password is entered. This prevents several trivial attacks, such as booting up from a floppy disk to run a program that extracts the Windows administrator password, to booting from an external hard drive to run a program that examines the internal hard drive. However, with enough time and access an attacker can easily bypass a BIOS password. The BIOS password can typically be reset by removing the internal battery or reconfiguring jumpers on the motherboard. This is one reason why the computer's case should be physically locked (recommendation 2.9). Some BIOS's also have known, hard-coded passwords.

We recommend:

1. All GEMS servers should incorporate a BIOS password conforming to the password selection and storage criteria described in section 3.1.

2. The BIOS should be configured to boot from the hard drive only.

3. The BIOS password should be changed anytime an authorized employee leaves the organization or disclosure is suspected.

4. Since there is only one BIOS password it must be shared among all authorized personnel that use the system. The password should not be shared with anyone else.

3.3 Windows Passwords

The next line of defense is the Windows logon password. As previously discussed, there are many weaknesses in the Windows OS that a knowledgeable attacker may exploit to gain administrator access to the machine. Consequently, the Windows OS should not be considered secure, especially if it has not been patched. Nevertheless, Windows passwords do afford some level of protection, particularly against less technical malicious insiders.

We recommend the following policies and controls for the Windows login account of the GEMS server:

1. All GEMS servers should incorporate a Windows password conforming to the password selection and storage criteria described in section 3.1.

2. Lock out the user account after three consecutive failed login attempts. This can be configured as a security policy in Windows.

3. All users should have their own login account. Users should never share accounts. Passwords must never be shared with anyone, not even a system administrator. These same recommendations are made by Diebold (Diebold Election Systems, January 11, 2007).

4. All users should change their password at least once every election cycle. This could be implemented with a yearly aging policy with a password history of 5.

5. An authorized user should never leave the server unattended after logging in. If possible, the machine should be powered off when all authorized employees leave the room.

6. Consider two-factor authentication (e.g. biometric fingerprint scanner in addition to a typed password).

3.4 GEMS Passwords

The GEMS database requires authentication with a username and password before the database may be accessed. Similar to the situation with Windows passwords, the GEMS database should not be considered secure even if an attacker does not have a valid GEMS username and password. The GEMS server is based on Microsoft Access, and many techniques exist in the public domain to exploit and manipulate the contents of an Access database. Nevertheless, GEMS database passwords do afford some level of protection, particularly against less technical malicious insiders.

We recommend the following policies and controls for the GEMS database passwords:

1. The database passwords should conform to the password selection and storage criteria described in section 3.1.

2. All users should have their own database account. Users should never share accounts. Passwords must never be shared with anyone, except when disseminated by the GEMS programmer to the GEMS regional supervisor that will use that account.

3. The practice of changing passwords every election cycle is adequate, given the relatively low frequency of use. However, care should be taken in the way that the GEMS databases are disseminated via CD-ROM. If an attacker intercepts the CD-ROM during transit it may be possible to incorporate malicious software with the contents of the database onto a new CD-ROM and then forward the compromised CD-ROM to the regional supervisor. If the compromised CD-ROM is inserted into the GEMS server then the server may be compromised.

   To mitigate this possibility we recommend that either:

   1. The databases be hand-delivered to the recipients.

      or

   2. A hash/checksum tool be run on the CD containing the database to be transmitted. The checksum would be communicated to the recipient by phone. When the recipient receives the CD-ROM it would be tested on a third machine to verify that the checksums match before inserting the CD-ROM on the GEMS server.

3.5 Other Recommendations

We also recommend the following practices and procedures that are related to password security:

1. If the physical security of a GEMS server has been compromised, password management is only a secondary concern. The Windows operating system is the weakest link due to the numerous security flaws that have been well documented and publicized. Many tools are readily available that allow attackers to quickly gain administrator privileges using known security flaws. To protect against many of these attacks, the GEMS servers should be patched with the latest Microsoft security updates. Use the procedure described in the Diebold Client Security document (Diebold Election Systems, January 11, 2007), section 4.1.1. This involves downloading the updates to a third computer, verifying their contents and checksums, then burning them onto a CD for installation to the GEMS server.

2. Disable any unnecessary services with the assistance of qualified IT personnel as described in the Diebold Client Security document (Diebold Election Systems, January 11, 2007), section 4.5.

3. Install and regularly update a malware detection program such as McAfee anti-virus software.

4. Evaluate the use a drive encryption program such as TrueCrypt or BitLocker (Windows Vista only) on the GEMS servers. This type of software encrypts/decrypts data stored on the hard disk in real-time. If an attacker removes the hard disk and attempts to mount it on a different machine, the data will be unreadable without the encryption keys.

5. Regularly inspect both Windows event logs and database logs for suspicious activity. The frequency of inspection should be on a fixed schedule and at a minimum include an inspection before, during, and after an election.

Appendix F: Ballot and Election Equipment Distribution and Chain of Possession

1 Ballot and Election Equipment Distribution and Chain of Possession

The process of holding a statewide election begins long before Election Day. The following section is a general description of the locations and movements of election ballots and voting machines through one election. Because Alaska communities are so diverse in their size and accessibility, there are exceptions to the processes not represented here. The state uses standard procedures to keep the process as consistent as possible, as we illustrate in several diagrams. Section 1.1 shows the icons used in those diagrams. We describe the creation and distribution of ballots both for hand counting precincts and for use in the optical scan voting machine (Sec 1.2); the general dispersion and return of the optical scan voting machines (Sec. 1.3) and touch screen voting machines (Sec. 1.4) from storage to the respective precincts and back to storage. The movements of the machines include the merging of memory cards with the voting machines and their removal and return to Juneau after the election.

With the large number of polling locations throughout Alaska, the distribution and storage requirements have always been a logistical challenge. For the majority of the life of any voting machine and memory cards, they reside in secure storage. From the beginning of an election cycle, there is the need to remove the machines from storage, test as appropriate, prepare, and distribute.

When ballots and voting machines are stored and when they are in transit there are challenges in protecting them from damage and the potential for unauthorized access. Accessibility, accountability, training, and documentation with regard to the chain of custody should be monitored and reviewed.

Icons Used in the Voting Process Diagrams

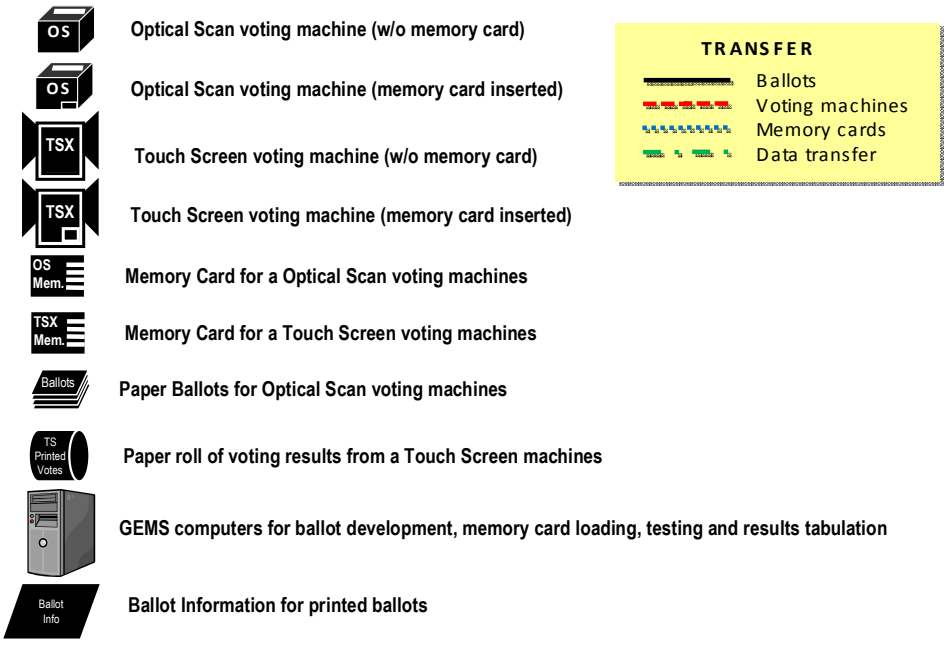


Figure 1 - Voting Process Diagram Icons

Optical Scan Ballots and Hand-Count Ballots

The following diagram and legend describe the movement between locations and over time for the optical scan ballots and the hand counted ballots between ballot design in Juneau (based on the candidates' applications filed with the Division of Elections) and other ballot issues. The regional election offices provide precinct-by-precinct official counts of registered voters and quantities of ballots needed for each voting location.

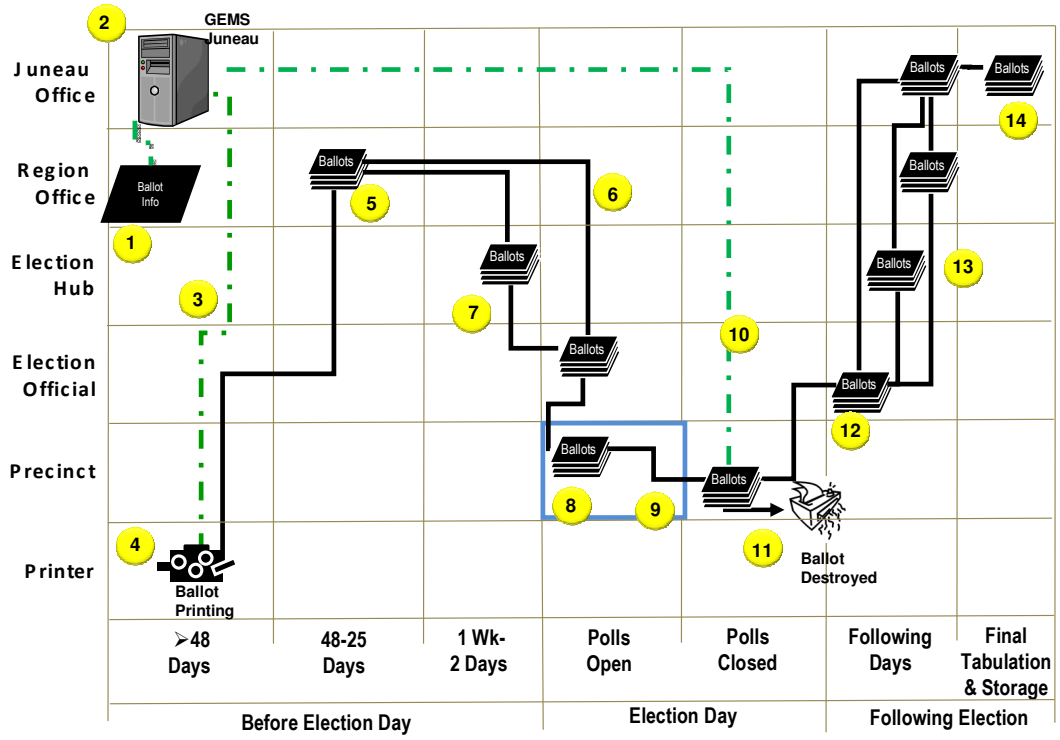


Figure 2 - Optical Scan Ballots and Hand-count Ballots – Chain of Possession

1. Regional offices submit the quantity of ballots needed for each voting location to the Director of Elections office in Juneau.
2. GEMS programmed with candidate information and layout.
3. Ballot information and precinct quantities are sent electronically to the ballot printer.
4. Ballots are sequentially numbered, printed and shrink-wrapped in quantities of 25.
5. Ballots are shipped by the printer to the Division of Elections offices in Anchorage, Fairbanks, Juneau, Mat Su and Nome.
6. Ballots for locations in rural Alaska are mailed by delivery confirmation to local election officials
7. Some locations ballots are shipped to hubs prior to distribution to election officials, while those locations within driving distance to a regional office picks up the ballots directly from the election supervisor.
8. Ballots are brought to polling places the morning of the election by an election official
9. After polls have closed all ballots are secured.

10. The OS voting machine transmits the results to Juneau. If hand counted, the results by the Regional offices to are called into Juneau. The unused ballots are destroyed.

11. The ballots are secured by the local election officials.

12. All ballots, along with signatures, memory cards and ballot statement are combined, sealed and returned to the Division of Elections. The route back is same as respective route ballots took to the polling places from a Regional Office.

13. All voted ballots are retained in Juneau for recounts and final archiving.

1.2.1 Optical Scan Machines (OS) and Memory Cards

Optical Scan machines are stored at Regional Election Offices or at selected hubs between elections. The memory cards for the Optical Scan machines are stored in Juneau between elections. After an election, OS machines are returned to their respective storage locations and the memory cards are all returned to Juneau for any necessary review and to be stored. Optical Scan machines, when in use, are locked in place on top of a black poly-carbon ballot box. These boxes are distributed separately and can be positioned at polling places before the morning of the election. They are designed to hold the scanned ballots and contain a side slot and separate chamber to hold any ballots voted but not scanned.

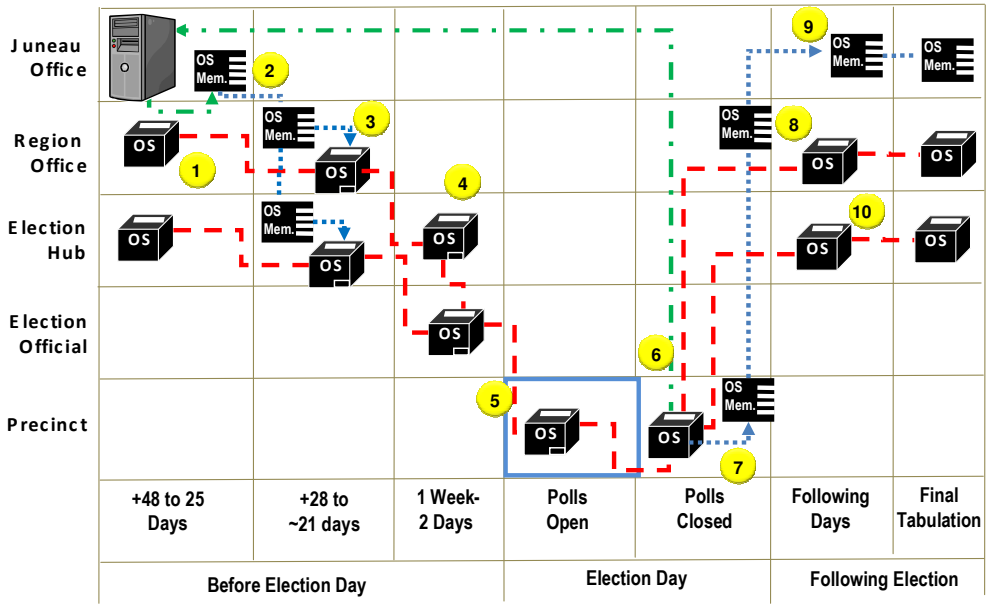


Figure 3 - Optical Scan Machine (OS) & Memory Card – Chain of Possession

1. Optical Scan Voting Machines (OS) are stored and tested at the Regional Offices or stored and tested at selected hub locations.
2. GEMS programs the memory card in Juneau. They are tested by the State Review Board there before being sent to the Regional Offices.
3. The memory cards and the OS machines are tested at the regional offices by the Regional Accu-Vote Board or in hub communities by Accu-vote coordinators.. The memory cards are inserted into the machines and sealed.
4. The OS voting machines are distributed to the precinct officials for placement on Election Day either from the Regional office or a hub.
5. The voting machines are placed at the precinct the morning of the election and are tested before the polls are open.
6. After the polls are closed, the ballot results are printed and signed-off by the election board and then are sent by the OS machine to GEMS in Juneau.
7. The memory card is removed and ballots, memory card, printed results and ballot statement are sent to Juneau either directly or through the Regional Office.
8. The memory cards are returned to Regional Offices when the cards can be delivered directly. Off the road system, cards are sent to Juneau directly.
9. The OS memory cards and printed results are received by the Juneau office for any needed review and final storage. At the Director's office, in Juneau the cards and printed results are used to resolve unexplained discrepancies.
10. The OS machines are returned to their originating Regional Office or hub for storage.

1.2.2 Touch Screen (TSX) Voting Machines and Memory

Touch Screen (TSX) voting machines must be available at each voting location to assist disabled voters who need special assistance. Electronically these are more sophisticated machines and are programmed with the ballot information both as a visual ballot and as an audible ballot for the blind. The TSX machine can be used by any voter, but are intended for use by disabled voters. As seen in the following flow diagram, as each voter votes, the machine produces a printed version of the voter’s choices, which the voter can see and confirm before casting a ballot. Once the ballot is cast on the TSX, the printed ballot is wound into a storage canister in the machine, which is removed after the polls close and returned along with the results stored in the memory card. The machines are returned to the locations where they are kept between elections. Because of the size and weight (60 lbs.) of the TSX machines, some are stored at communities between the primary election and the subsequent general election.

The printed records from TSX machines are treated as “official” ballots for their return to regional offices and to Juneau. Likewise, the TSX memory cards are treated like the memory cards from the OS machines.

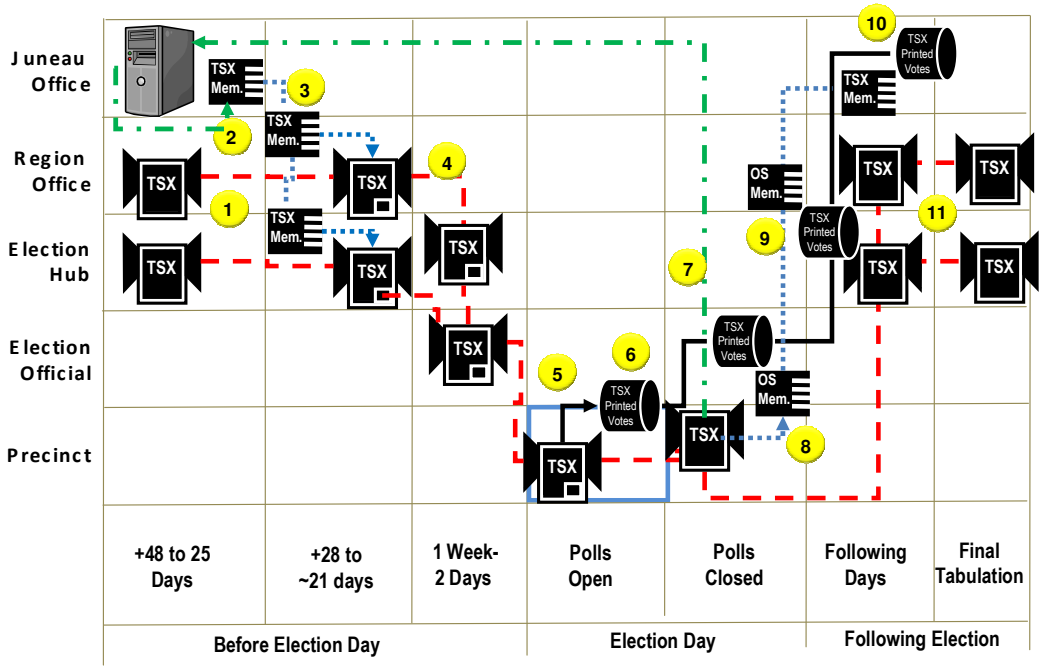


Figure 4 - Touch Screen (TSX) Voting Machine & Memory Card – Chain of Possession

1. Touch Screen Voting Machines (TSX) are stored and tested at the Regional Offices and at selected hub locations.

2. GEMS programs the TSX memory card in Juneau. They are tested there by the State Review Board before being sent to the regional offices.

3. The memory cards and the TSX machines are tested at the regional offices by the Regional Accu-Vote Board. For those machines stored in hub locations, the memory card is sent to the hub location. The memory cards are inserted, either at the regional office or hub location, into the machines and sealed before being distributed.

4. The TSX voting machines are distributed to the to precinct election officials for placement on Election Day.

5. One TSX voting machine is positioned at each of the polling places for use while the polls are open.

6. As voters use TSX voting machines, their choices are printed onto an enclosed printed roll. The voter can review and confirm their choices on the printed version of the ballot. Upon approval, the results are reeled into a container within the machine and stored. The individuals' results are also stored on the memory card in the AV-TSX machine.

7. After the polls are closed, the final results are both printed from the AV-TSX machine and the results are transmitted electronically to GEMS in Juneau with t he exception of results in hand-counted precincts and those that are called in to Regional offices and up-loaded to Juneau.

8. The memory card, printed ballots, printed results summary are removed after the polls are closed and the AV-TSX machine's results are transmitted.

9. The AV-TSX memory cards are returned to the Regional offices or hub for delivery to Juneau or in some cases sent directly to Juneau..

10. The memory cards and the printed AV-TSX ballots rolls are returned to Juneau for review and, in the case of the ballot rolls, archiving.

11. The AV-TSX machines are returned to the Regional Office or hub where they originated for storage.

The information regarding movements is general. Actual movements between the beginning and end of an election cycle can be quite complex.

Premier Election Solutions

California Tamper Evident Security Seal Document

Version 2
January 17, 2008

Premier Election Solution
Tamper Evident Security Seal Document

The following document illustrates the recommended placement of tamper evident security seals on Premier Election Solution (Premier) equipment. The applicable equipment includes the AccuVote-OS (optical scan) and the AccuVote-TSX (touch screen). Premier is using best practices on the placement of security seals based on discussions and interviews with several California counties. The placements of those seals are recommendations to mitigate any potential tampering of the AccuVote-OS and AccuVote-TSX units.

Counties are recommended to use this placement of seals, along with augmenting the security seal placements with additional placement of seals on the voting equipment, depending on the county's security seal policies and procedures. The recommended placement of seals on the unit should not preclude a county from continuing to utilize their best practices regarding seal placements on the AccuVote-OS and AccuVote-TSX units.

Premier is illustrating where the placement of the security seals could be placed on those units. As far as the actual security seals, Premier does not recommend a specific vendor. However, tamper evident security seals from vendors such as Intab and Seton have been used on the equipment with success. There are illustrations of those seals within this document.

All seals used on Premier equipment should be serialized and tamper evident. Additionally, the security seals must be logged and tracked by the authorized election officials and verified by the poll workers prior to using the voting equipment. This verification process ensures the equipment has been thoroughly checked and verified against any potential tampering of those units

In some seal application areas, a choice of different seal types is available. In other instances, the choice to apply multiple seals is possible. The following outline pictures will demonstrate the use and location of wire anti-tamper evident labels, wire seals, plastic (rat tail) seals, and spring lock seals on the AccuVote-OS and AccuVote-TSX.

The following is a list of the seal application areas by the equipment type. The equipment type also includes the AccuView Printer Module (AVPM) which contains a security canister used for housing the voter-verifiable paper audit trail. The AVPM security canister is secured using a spring lock security seal or a tamper evident security seal.

Seal Application Areas by Equipment Type

- AVOS
  - Memory Card seal
    - Wire Security Seal

- AVTSX
  - Memory Card Slot seal
    - Anti-Tamper Evident Security Seal Label

- AVTSX Front Panel Door seal
  - Wire Security Seal
  - Plastic (rat tail) Security Seal

- AVPM
  - Printed Receipt Security Canister Seal
    - Spring Lock Security Seal
    - Anti-Tamper Evident Security Seal Label

There are several types of tamper-evident seals and labels used on the AccuVote-OS and AccuVote-TSX units. The following seals have been used on the AccuVote-OS and AccuVote-TSX security seals. The wired and spring lock seals have been used for the memory card slot on the AccuVote-OS unit. The tamper evident security seals and spring lock seals have been utilized on the AccuVote-TSX units.

Wire Security Seal (Passive RFID Tool less Roto Tag)

Spring Lock Plastic Security Seals (Heat Stamped and Consecutive Numbering)

Tamper Evident Security Seals Label (1 by 3 inches, serialized)

Tamper Evident Security Seal Label (1 by 3 inches, bar-coded and sequential numbered)

Tamper Evident Security Seal (10 inch pull tight seal, Heat stamped and serialized)

AccuVote-OS Security Seal Locations

The following are recommended locations for the placement of security seals on the AccuVote-OS unit. Counties are recommended to use this placement of seals, along with augmenting the security seal placements with additional seal placements, depending on the county's security seal policies and procedures. The recommended placement of seals on the unit should not preclude a county from continuing to utilize their best practices regarding seal placements on the AccuVote-OS. At a minimum, a jurisdiction should seal the following locations on the AccuVote-OS unit when used in the precincts:

- Memory Card Slot
- Sealed over the front of the AccuVote-OS unit over the "seam" on the AccuVote-OS unit, and / or in the rear of the AccuVote-OS unit over a screw hole as well as over the "seam" on the back of the AccuVote-OS unit

All of the security seals must be logged, serialized and verified by the poll worker prior to using the equipment on Election Day. The jurisdictions could deploy a seal verification log which the poll worker could verify the security seal with the seal verification log document.

See the photos below for an illustration of the security seals on the AccuVote-OS.

AccuVote-OS Memory Card Slot Sealed with a Security Seal

AccuVote-TSX Security Seal Locations

The following are recommended locations for the placement of security seals on the AccuVote-TSX unit. Counties are recommended to use this placement of seals, along with augmenting the security seal placements with additional seal placements, depending on the county's security seal placement policies and procedures. The recommended placement of seals on the unit should not preclude a county from continuing to utilize their best practices regarding seal placements on the AccuVote-TSX. At a minimum, a jurisdiction should seal the following locations:

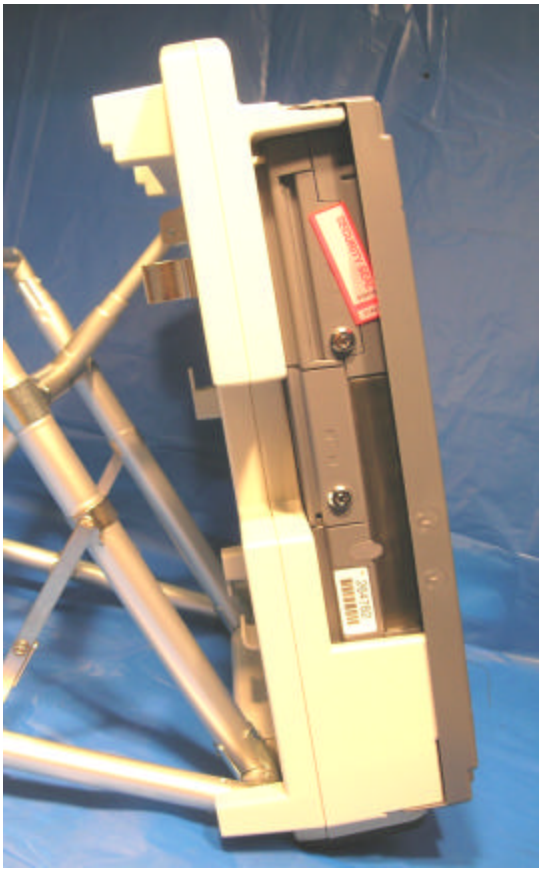
- AVTSX Memory Card Slot and /or On/Off Slot
- On the AccuVote-TSX over a screw hole, which would also cover the "seam" on the AVTSX unit

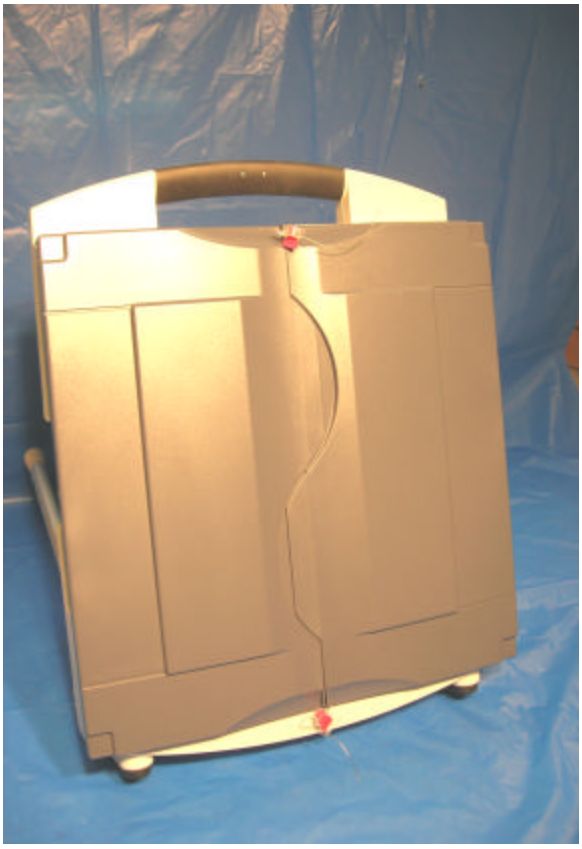
Additionally, a security seal should be placed sealing the AccuVote-TSX "doors".

All of the security seals must be logged, serialized and verified by the poll worker prior to using the equipment on Election Day. The jurisdictions could deploy a seal verification log which the poll worker could verify the security seal with the seal verification log document.

See the photos below for an illustration of the security seals on the AccuVote-TSX.

Illustration of AccuVote-TSX Security Seal Placements



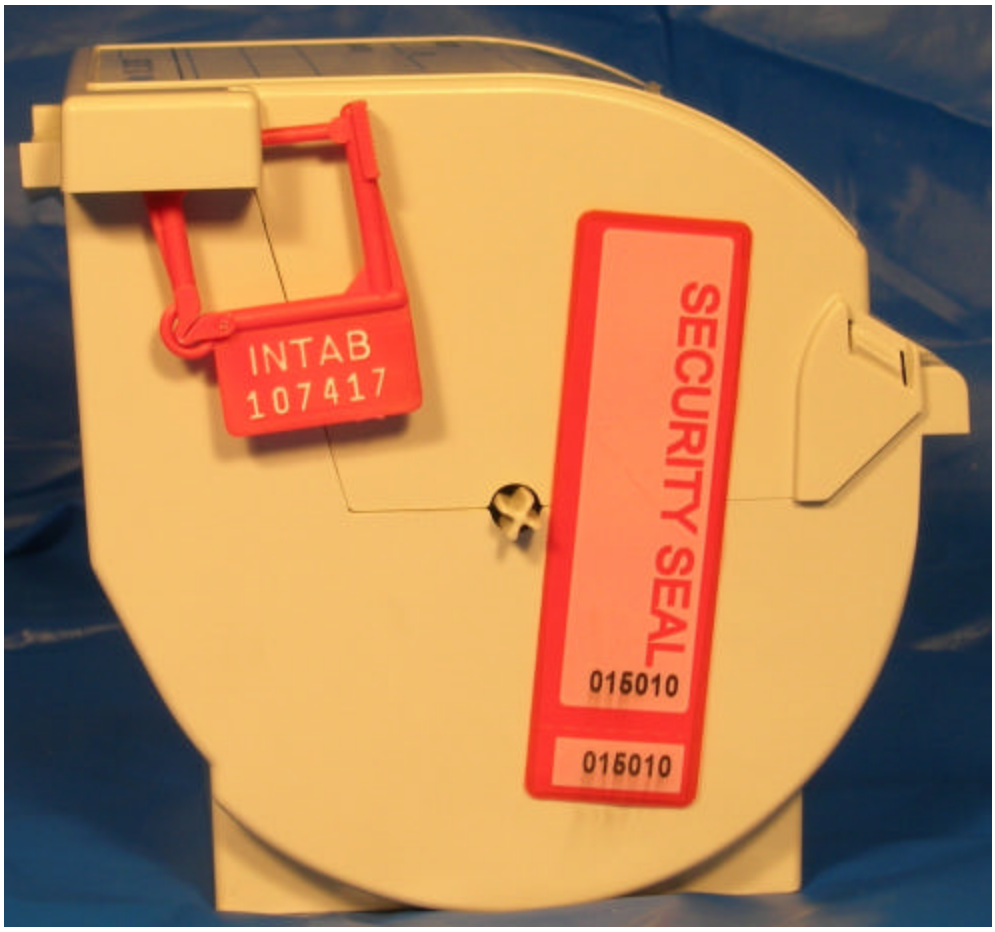


AccuView Printer Module (AVPM) Security Seal Locations

The following are recommended locations for the placement of security seals on the AVPM. At a minimum, a jurisdiction should seal the following locations:

- On the AVPM security canister with a tamper evident security seal sealed over the opening of the AVPM security canister; or
- With a springlock seal on the security canister

The security seal needs to be placed on the security canister when the security canister has been fed with paper, and the security canister has been closed. See the photos below for an illustration of the security seals on the AVPM.



Appendix H – Security Training

General instructions to poll workers

To ensure 5 votes on AV-TSX poll workers vote at the end of the day. Poll workers should vote at the end of the day. If there are more than 1 but fewer than 5 votes cast on AV-TSX, then they should cast their votes on AV-TSX machines.

Tampering doesn't need to be sophisticated. Attempts at election fraud can look more like vandalism that high tech computer hacking. If someone is worried about losing an election in specific precinct, that person might try to prevent people from voting for opponent by causing a disruption.

Election results would also be destroyed if someone spilled liquid on to the AV-TSX printer. The printer paper absorbs liquids, so a spill could leak though plastic cover and absorb into the paper on the spool.

Don't allow loitering in the area around voting booths.

Don't allow people to bring food or beverages into voting booths.

Equipment used in absentee voting locations is exposed to tampering for several days. People in charge of elections in absentee locations need to exercise vigilance and ensure that voting equipment is locked in secure storage areas when a voting official is not present.

Tamper evident seal inspection on AV-TSX and AV-OS machines

Regional Offices

Prior to election

1. Prior to opening polls. Keep list of all machines/precincts where poll workers have reported that tamper-evident seals have been broken.
2. After election. Test and inspect memory cards from machines where seals have been broken. Votes cast on these machines may be subject to 100% manual tally.

Precincts

Prior to opening polls

1. Prior to opening polls. Inspect tamper evident seal on the AV-TSX machine. DO NOT REMOVE SEAL.
2. If seal is not broken, check "no" on checklist.
3. If the seal is broken, check "yes" on the checklist and notify Regional Director.

Appendix I – AV-OS Shipping Container Example

1 Description

The AccuVote optical scan (AV-OS) machines currently use cardboard boxes with hard cell foam inserts. These cardboard boxes are prone to deterioration over time, especially when considering the frequency use they receive. An assessment of the reliability of the AV-OS machines found a measurable number of AV-OS repairs required resulting from physical damage incurred during shipment or transport.

An improved shipping container would reduce the number of failures due to physical damage during shipment and transport. Initial procurement of new shipping containers requires the purchase of a new case for each AV-OS machine. The cases purchased for use in the shipment of AV-OS machines would make suitable, robust storage containers as well, further protecting the devices from damage. The selected shipment and storage container should allow the Division of Elections to lock the case with a tamper seal.

2 Example Case and Cost Estimate

The dimensions of the AV-OS machine are 16 inches X 14 inches X 3 inches. These dimensions can be accommodated by a Pelican™ Products 1600 series case. The 1600 series case has interior dimensions of 21.43 inches X 16.50 inches X 7.87 inches. Pelican™ 1600 cases are watertight, crushproof and dust proof making them ideal for transport and storage of sensitive electronic equipment. Custom configurable foam interior lining allows the case to be fitted to the AV-OS machine. Pelican™ cases also include openings for case security (lock or tamper seal insertion).

It is recommended that the Pelican™ 1600 case or a similar product is purchased for the storage and transport of all AV-OS machines owned by the Division of Elections.

The Pelican™ 1600 case is available at an average street price of $160. The Division of Elections has a total of 290 AV-OS machines in its possession. This results in a total cost of approximately $46,400.00 to procure new cases. In addition to the procurement cost there is labor associated with configuring each case for the AV-OS machines. An estimate of 30 minutes per case to configure the foam lining results in a labor estimate of 145 man hours.

A manufacturer cut sheet taken from the Pelican™ Products website is included on the following page.

Print | Close Window

Uncontrolled document as of April 28, 2008. Refer to website for up to date specifications.

CASES 1600 Case

1600 Case

- Watertight, crushproof, and dust proof
- Open cell core with solid wall design - strong, light weight
- Automatic Pressure Equalization Valve
- O-ring seal
- Comfortable rubber over-molded handle
- Stainless steel hardware and padlock protectors
- 2 level Pick 'N' Pluck™ with convoluted lid foam
- Personalized nameplate service available
- Unconditional Lifetime Guarantee of Excellence

1600 Case Configurations

Cat. #	Description
1600	1600 Case
1600NF	1600 Case (No foam)
1604	1600 Case with Padded Dividers

 Black
 Silver
 Orange
 Yellow
 OD Green*
 Desert Tan

*OD Green available upon request

1600 Case Specifications

Exterior Dimensions (L x W x D)
24.25" x 19.43" x 8.68" (61.6 x 49.3 x 22 cm)

Interior Dimensions (L x W x D)
21.43" x 16.50" x 7.87" (54.4 x 41.9 x 20 cm)

Lid Depth
1.75" (4.4 cm)

Bottom Depth
6.12" (15.5 cm)

Total Depth
7.87" (20 cm)

Weight with Foam
14.11 lbs. (6.4 kg)

Weight without Foam
13 lbs. (5.9 kg)

Buoyancy Max.
74.96 lbs.
(34 kg)

Range Temperature
-10 / 210° F
(-23 / 99° C)

Personalized Nameplate Available

1600 Case Certificates

• IP67 (1 meter submersion for 30 minutes)
• MIL C-4150J • Def Stan 81-41/STANAG 4280 • ATA 300

1600 Case Accessories

Cat. #	Description	Sug. Retail
1600IP	Instapak Quick® RT	US$47.95
1601	4 pc. Replacement Foam Set	US$99.95
1602	Pick 'N' Pluck™ Sections Only (set of 2)	US$81.95
1603	Replacement O-ring	US$5.25
1605	Padded Divider Set Only	US$158.95
1609	Lid Organizer	US$45.95

Appendix J - AccuVote Communications System Description

1. Introduction

The purpose of this document is to analyze and document the configuration and topology of the State of Alaska Division of Elections AccuVote communications network. The goal of this analysis is to identify any potential vulnerabilities and to recommend enhancements to the Division of Elections.

2. Network Topology

The Division of Elections (DoE) AccuVote communications network is utilized to transmit preliminary, unofficial election results to the DoE director's office host GEMS upon the close of polls at each precinct. These results are tabulated by the director's office GEMS and are provided as preliminary, unofficial results to the public.

The Division of Elections AccuVote communications network is comprised of the following network transmission types.

1. AccuVote Optical Scan (AV-OS) and AccuVote Touchscreen (AV-TSX) Precinct Reporting

Each voting precinct utilizing AV-OS and AV-TSX machines reports preliminary results using an internal modem which is fully tested prior to each election. The internal modem is connected to a local Public Switched Telephone Network (PSTN) jack at the precinct. Using the public telephone network a communications channel is established between the DoE director's office GEMS server and the local precinct equipment. A total of 48 analog modems in the director's office are configured to handle the incoming requests as precincts are closed across the State of Alaska.

The AV-OS and AV-TSX machines are configured to utilize the Secure Socket Layer (SSL) protocol to ensure that the communications channel is secure. Use of this protocol minimizes eavesdropping vulnerabilities over the communications channel.

2. GEMS Handcount Reporting

The regional office GEMS servers are used following an election to enter handcount ballots into the AccuVote system. The handcount ballots are collected and a data entry technician enters the ballots into the region's GEMS software. When all of the ballots have been captured in the GEMS server the ballots results are transmitted to the GEMS in the DoE director's office in Juneau using an analog modem.

Ballot results transmitted in this manner are connected to PSTN in the same manner as the precinct AV-OS and AV-TSX machines. In the case of Region 3 the PBX is interconnected using a dedicated T-1 circuit provided by the telecommunications carrier General Communication Inc. An option 81 Nortel PBX located in the Juneau, Alaska director's office terminates all transmissions into the DoE director's office.

A total of 6 regional GEMS servers are used in each election to enter handcount ballots. The GEMS servers are allocated based on the number of handcount precincts present in a region. A regional breakdown of the number of handcount precinct as well as the number of regional GEMS servers is provided below.

Region	Handcount Precincts	GEMS Servers
Southeast – Region 1	18	1
Anchorage and Matsu – Region 2	1	1
Fairbanks and Interior – Region 3	45	2
Nome, Barrow, West Coast – Region 4	85	2

Each regional GEMS server is configured to utilize the Secure Socket Layer protocol when transmitting data between itself and the DoE director's office GEMS.

3. Recommendations

The current Division of Elections communications network appears to be implemented in a reasonable, robust manner. Built-in safeguards such as implementation of the SSL protocol are in use as suggested by Premier Election Solutions.

The State of Alaska Election Security Project was made aware that the State of Alaska will be transitioning its current analog phone system to a full voice over IP (VoIP) system in the future. It is recommended that a subsequent analysis of this network be performed once the details of the new voice network are finalized. Implementation of a VoIP network presents a different set of security risks to data transmission and these risks and vulnerabilities should be assessed before the network is used for a subsequent election.

Daisy Chain Serial Server Connection

Active GEMS Server

SSL

SCSI

Digiport 16EM Serial Server

Digiport 16EM Serial Server

Digiport 16EM Serial Server

Multitech Rack Mount Modem 16 Each T5600BR-V92

Multitech Rack Mount Modem 16 Each T5600BR-V92

Multitech Rack Mount Modem 16 Each T5600BR-V92

16 Port NT8D09

16 Port NT8D09

16 Port NT8D09

Backup GEMS Server

Juneau Director's Office

Nortel Option 81 Private Telephone Exchange (PBX)

Private Line Circuit

Public Switched Telephone Network

Analog Modem

SSL

handcount ballots (18 Precincts)

GEMS Server

SSL modem **AV-OS (71 Precincts)**

SSL modem **AV-TSX (89 Precincts)**

Voting Precincts

Region 1 Southeast

Analog Modem

SSL

handcount ballots (1 Precinct)

GEMS Server

SSL modem **AV-OS (151 Precincts)**

SSL modem **AV-TSX (152 Precincts)**

Voting Precincts

Region 2 Anchorage and Matanuska Valley

handcount ballots (85 Precincts)

SSL

Analog Modem

GEMS Server

SSL

Analog Modem

SSL

GEMS Server

SSL modem **AV-OS (12 Precincts)** SSL

SSL modem **AV-TSX (97 Precincts)** SSL

Voting Precincts

Region 4 Nome, Barrow and West Coast

Private Telephone Exchange (PBX)

Analog Modem

SSL

GEMS Server

Analog Modem

handcount ballots (45 Precinct)

SSL

GEMS Server

SSL modem **AV-OS (56 Precincts)**

SSL modem **AV-TSX (101 Precincts)**

Voting Precincts

Region 3 Fairbanks and Interior

State of Alaska
Election Security Project

DoE AccuVote Network Topology			
Name:	AccuVote Election System Network Interconnection Topology		
Drawn By:	Mark Ayers	Date:	*4/13/2008*
Edited By:		Edited:	
Scale:	*NTS*	Sheet:	*1 of 1*

Appendix L - AccuVote Reliability Assessment

1. Introduction

This document assesses the reliability of the AccuVote system components operated by the State of Alaska Division of Elections. The Division of Elections maintains records of AccuVote Optical Scan equipment that is returned to Premier Elections Systems for repair with varying detail by region. These records provide information regarding the failure mode and the repairs required to return the machine to "as new" condition. Records regarding the AccuVote Touch Screen and GEMS systems are not maintained in sufficient detail to evaluate reliability trends.

This document describes the reliability requirements as stated in the Voting System Standards (VSS) 2002 (2002) specification and describes the concept of reliability as it relates to the Division of Elections' system. A brief discussion of the VVSG Recommendations to the EAC (2007) is provided as this document provides a significant improvement in the specification of reliability performance regarding electronic voting systems over the 2002 VSS. An evaluation of the limited data set provided by the Division of Elections offers some insight regarding the failure trends and observations. Recommendations are made regarding ways to improve the reliability and performance of the AccuVote Optical Scan hardware.

2. Reliability Performance Specifications

The reliability performance required from the AccuVote hardware and software is defined in the Federal Election Commission's 2002 Voting Systems Standards. Conformance with these specifications is required by state aw. Conformance with these specifications is established through the Independent Testing Authority (ITA) certification process. The 2002 VSS uses the term "system" in several instances when discussing both reliability and availability.

Taken in the context of the 2002 VSS, the term "system" can be taken to imply a single voting machine under test. This is consistent with the ITA test report results. It is our opinion that this interpretation is inconsistent with commonly accepted reliability theory and that the values specified by the 2002 VSS result in reliability certifications which are of little value to the Division of Elections. Reliability and availability are statistical quantities and must be taken in the context of a statistically significant volume of machines or units. In the case of the State of Alaska this would mean considering a system which is sized at least as large as one of Alaska's four regions. Further discussions in this section which use the term "system" will clarify whether the intent is to indicate a single voting machine (hardware and software) or a set of voting machines.

The minimum reliability and availability required for certification in the State of Alaska are specified in the 2002 VSS.

Reliability is defined in the 2002 VSS in terms of the statistical parameter mean time between failures (MTBF). This parameter defines the average interval between which failures occur. A failure is defined as any event where the system (an individual machine or set of machines) fails to perform one or more functions or exhibits behavior where performance is degraded to an unusable condition for a period of greater than 10 seconds. The MTBF is defined in the 2002 VSS as having a minimum value of 163 hours.

System availability is the probability that the system performs the desired functions at any instant in time under stated conditions. The VSS 2002 standard provides guidelines for both the

calculation and evaluation of the system availability. Specific system components are required to meet availability specifications within the VSS 2002 guidelines. In the case of the AccuVote optical scan (AV-OS) machines the functions of voter selection recording and paper ballot encoding must meet the availability requirement. The AccuVote touch screen (AV-TSX) availability requirement applies to the recording and storage of voter ballot selections. In both the AV-OS and AV-TSX cases the consolidation of the vote data requires that the Global Election Management System (GEMS) also meet the availability requirement. The VSS 2002 standard specifies a minimum system availability of 99%.

Upon reviewing the ITA certifications documents the evaluation of reliability and availability are subject to interpretation and do not seem to provide useful performance measures. Review of the Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission (2007) specification provides a significant change in the performance specifications associated with voting system reliability. This specification has not yet been ratified and is not in force for the State of Alaska. A review of its contents is valuable for the assessment of future voting system performance specifications and evaluation of those changes against the system currently in operation.

3. Division of Elections System Performance

Evaluation of the Division of Elections system using empirical data is problematic. Comprehensive records regarding failures of the AV-OS, AV-TSX and GEMS system components do not exist. As such the statistical data here is based on records kept by Region III (Fairbanks) and Region IV (Nome, Barrow, West Coast of Alaska). Qualitative information can be gleaned from these records regarding AV-OS and AV-TSX performance weaknesses and areas in which improvements might be made.

3.1 System Description

The State of Alaska Division of Elections operates a Premier Election Solutions AccuVote system with the following AccuVote component counts. The counts presented in Table 1 refer to precinct counts. The Division of Elections maintains additional AV-OS and AV-TSX machines as spare units in the case of a failure.

Region	AV-OS	AV-TSX	GEMS
I - Southeast Alaska	71	89	1
II - Anchorage / Mat-su	151	152	1
III - Fairbanks / Interior	56	101	2
IV - Nome / Barrow / West Coast	12	97	2
Juneau Director's Office	0	0	2
Total	*290*	*439*	*8*

Table 1. AccuVote System Component Count by Region

The GEMS servers in the Juneau Director's office operate in a redundant configuration where a backup server available in the case that a failure of the primary server occurs. This backup server is configured prior to each election to exactly mirror the configuration of the primary GEMS server. In the case that the primary GEMS server fails the backup server would quickly be brought into service. A minimal service outage would result in the case of a primary GEMS server failure. Redundancy for the backup server is not provided.

Precinct level machines are operated in a non-redundant configuration. Two different deployments of AV-OS and AV-TSX machine are used depending on the population of each community. In larger communities a single AV-OS and AV-TSX is allocated to each voting precinct. Smaller communities utilize hand-counted paper ballots or optional use of the AV-TSX machines.

A non-repairable failure of the AV-TSX voting machine results in voters being directed to use the AV-OS machine in that precinct (where available). Failure of the AV-OS machine results in a precinct hand count. The paper ballot reliance built into the Division of Elections system results in a system in which no failure can occur which would cause a voter to be turned away during an election.

During live elections the Division of Elections employs “rovers”. Rovers are trained on-call helpers responsible for assisting with trouble calls during an election. They are trained to replace malfunctioning equipment and to assist election workers in ensuring that the election hardware works properly on election day. Rovers serve to increase the availability of AV-OS and AV-TSX machines by reducing the equipment outage duration associated with a failed component in urban areas. Rovers are employed by the Division of Elections in Anchorage, Fairbanks, Juneau, Kenai Borough, Sitka, Kodiak, Valdez, Nome and the Matanuska Valley. In all other communities the failure of an AV-OS or AV-TSX results in it being removed from service and the ballots hand counted.

Although a rigorous academic reliability analysis of the Division of Elections AccuVote system does not exist for public review the historical performance of the system is very good. The Division of Elections reliance on paper ballots as the final ballot of record ensures that in no circumstance will a voter be turned away because of equipment malfunctions. Failures of system components result in an increase in election worker resource requirements but do not affect the outcome of an election.

3.2 Premier Election Solutions Reliability Models

The VSS 2002 standards set specific requirements regarding the reliability and availability of election systems (as defined in the 2002 VSS). Certification of the AccuVote system used by the Division of Elections against the VSS 2002 standard ensures compliance with the reliability requirements. Section 3.4.5 of the VSS 2002 requires vendors to specify the configuration of systems to the ITA for evaluation. This configuration specification includes sparing recommendations, maintenance / repair staffing recommendation and system configurations required to ensure that the required availability is met.

Unfortunately, the content of these technical details remains closed to public disclosure and these documents were not reviewed as part of this analysis.

3.3 Division of Elections Failure Data

The State of Alaska Division of Elections has maintained repair and maintenance records for the AV-OS machines in Region III (Fairbanks and Interior) and Region IV (Nome, Barrow and West Coast of Alaska) of the voting system. These records were reviewed and the primary failure modes were determined.

Repair records for Region III and Region IV are not in the same format and as such the resultant analysis is qualitative in nature.

Region III maintenance and repair data provided to the SOAESP team records repair activities for the AV-OS machines dating back to 1998. A total of 37 failures are recorded in the Region III AV-OS repair records between 1998 and 2006. It was recorded that four (4) of the failures were coincident with physical damage to the machine. In many cases the machines housing was cracked or damaged and had to be replaced.

Failure Mode	Number of Failures
Ballot Reader	21
Modem	7
Liquid Crystal Display	4
Power Supply	2
No Trouble Found by Premier	5
Printer	0

Table 2. Region III AV-OS Failure Modes

Review of this data shows that the AV-OS ballot reader is the primary component failure mode. The percentage of failure column in Table 2 does not sum to 100% because in several instances a multiple failure was discovered during the repair of the AV-OS machine. During the period between 1998 to 2006 a total of 28 unique machines failed in a manner requiring repair by Premier Election Solutions. Table 1 indicates that in Region III 56 AV-OS machines are in use which results in the unique failure of exactly 50% of AV-OS machines in the 1998 to 2006 time period.

Region IV maintenance and repair data provided records of the maintenance activity for both the AV-OS and AV-TSX machines over the time period from 2000 to 2007. Failure data for the 17 AV-OS machines in Region IV are provided in Table 3.

.

Failure Mode	Number of Failures
Ballot Reader	7
Modem	1
Liquid Crystal Display	0
Power Supply	2
Printer	1

Table 3. Region IV AV-TSX Failure Modes

Failure data from Region IV confirms that results seen in the Region III data indicating that the ballot reader is the least reliable component in the AV-OS machine.

Failure data for the 102 Region IV AV-TSX machines is provided in Table 4.

Failure Mode	Number of Failures
Printer	7
Modem	4
Screen	2
Enclosure	4
Memory Card Slot	1

Table 4. Region IV AV-OS Failure Modes

The data in Table 4 shows that printer failure is the primary mode of failure for the AV-TSX machines.

4 Recommendations

Review of the Division of Elections empirical data log with the 2002 VSS and 2007 VVSG indicate a high operational reliability and availability for the AccuVote system in the State of Alaska. The specifications provided by the 2002 VSS certification provide little insight or value regarding an AccuVote system consisting of hundreds of machines which operate simultaneously during an election. In spite of an apparent lack of publicly available academic rigor regarding reliability and availability of the system operated by the Division of Elections the practical reliability and availability are extremely high.

The reliance on the paper ballot as the final ballot of record provides an inherent improvement in system reliability which could never be achieved in a system which exclusively uses Direct Recording Electronic (DRE) voting terminals. Failure of electronic components in the current Division of Elections increases the resource dependence by initiating the hand count process but no time jeopardizes a precinct's ability to serve voters.

Although the current system is very robust and effective, we are making recommendations which should prove to incrementally reduce machine maintenance and improve reliability. More robust functional and logic and accuracy testing as detailed in Appendices M and N are recommended. Increased functional testing scope would serve to better detect hardware failures prior to equipment shipment and will reduce day of election field failures.

Better storage and transport containers for AV-OS are also recommended. Empirical maintenance data review indicates a measurable number of AV-OS machines experiencing physical damage during shipment and transport. The correlation between the transportation of the AV-OS machines and their failure rate was not reviewed as part of this analysis but it also recommended if improved transportation packaging for the AV-OS machines does not result in a reduction of machine failures. Vibration, environmental effects and contamination are all likely to contribute to an increased machine failure rate.

Appendix M - AccuVote Functional Test Guidelines

1. Introduction

The purpose of this document is to outline a set of recommended functional tests to be performed as part of pre-election and precinct testing for each AccuVote Optical Scan (AV-OS), AccuVote Touchscreen (AV-TSX) machine, Voter Card Encoder and GEMS server in preparation for deployment during an election cycle.

This document is organized into two sections. The first, "Current Functional Tests" outlines the current functional tests performed by the Division of Elections prior to deployment of the AV-OS, AV-TSX, and Voter Card Encoder devices in each precinct for an election cycle. The second section "SOAESP Recommended Functional Tests" details an expanded set of functional tests recommended for implementation. This expanded set of functional tests provides a more comprehensive functional check prior to each election cycle potentially reducing the number of election system failures in the field on election day.

2. Current Functional Tests

Currently the Division of Elections performs functional testing on the AV-OS platform prior to deployment for each election cycle. The AV-TSX platform is subjected to Logic and Accuracy testing but documentation received by the SOAESP project team does not indicate functionality testing before each election cycle. In addition, no documentation indicates functional testing on the Voter Card Encoder or GEMS server election system components. Section 3 of this document outlines recommended functional tests for these components.

2.1 AV-OS Physical Test

2.1.1 Physical damage to unit check.
The AV-OS machine is physically inspected for damage prior to use. Specific damage to identify is not called out in the test procedure.

2.1.2 Printer door lock test
The door lock to the AV-OS printer compartment is checked to ensure that the lock is functional and that the key works in the lock.

2.1.3 Serial number or State of Alaska tag number recording
The serial number or State of Alaska tag number is recorded at the top of the functional test document.

2.1.4 LCD readability test
The AV-OS is tested to qualitatively confirm that the LCD is readable and that the entire LCD component has not failed.

2.2 AV-OS Vote / Modem Testing (Regional Offices)

In addition to the physical test set specified by the Division of Elections an additional set of tests focused on verifying modem connectivity between the AV-OS and the GEMS is also conducted.

Upon startup of the AV-OS in pre-election mode the AV-OS supervisor or central administrator follows a set of prompts within the system to perform a series of tests on the AV-OS machine.

Test Ballots

The AV-OS vote test verifies that the ballot counting functionality is working properly. This test does not include the validation of un-voted or fully voted ballots. Upon completion of the ballot count test the user instructs the AV-OS system to print the test results in short form.

Modem Transmission Test

The user follows the LCD prompts, validates the phone number in the AV-OS and transmits the results by telephone to the modem bank connected to the GEMS server in the Juneau Division of Elections director's office. The AV-OS transmits the dummy data and the modem transmission test is completed.

Comments

The Vote / Modem Testing procedure currently in use by the Division of Elections provides a very basic functional check of two portions of the AV-OS system. These checks confirm ballot counting (not tabulation) and modem functionality.

The AV-OS system provides a suite of tests that should be considered by the Division of Elections to decrease the probability of discovering a failed component or system on the AV-OS machine on election day. We recommend a test suite for consideration by the Division of Elections detailed in Section 3 of this document.

3. SOAESP Recommended Functional Test Procedure

3.1 Election Functional Test Lifecycle

The recommended functional tests are broken into two different groups. A set of functional tests is recommended to be performed at the Regional Center prior to precinct shipment. Upon arrival at the precinct it is recommended that a subset of these test be re-performed to ensure reliable functionality on voting day.

Precinct tests are intended to be performed at the precinct immediately prior to the election and their purpose is to validate the hardware for use on election day. The Regional Office tests are more comprehensive and are intended to identify any issues with a machine before it is distributed to the precinct for use in the election.

A checklist should be provided to each Regional Center. This checklist (similar to the one currently in use by the Division of Elections) would be filled out and returned with the AV-OS machine at the end of the election. Anomalies or comments should be included on the

checklist sheet to identify any issues arising from the tests. Each checklist should be scanned at the end of the election and logged electronically to a common location for each machine to create a functional checkout history of the machine.

A sample functional test lifecycle for AV-OS and AV-TSX machines is provided below.

1. Election cycle checklist is generated for each voting machine (AV-OS and AV-TSX).
2. Functional testing is performed for each AV-OS and AV-TSX machine at the Regional Center level. (This does not necessarily imply that the test itself must be performed physically at the Regional Center).
3. The functional test checklist document is filled out by the Regional Center level technician.
4. The AV-OS or AV-TSX machine is boxed and readied for shipment with the functional test checklist included in the box.
5. Functional testing is performed for each AV-OS or AV-TSX machine at the Precinct level prior to election administration for each election (Primary and General). The functional test checklist document is further updated with the results of the precinct level test for the Primary and General elections.
6. The election is conducted.
7. The functional test checklist document and AV-OS or AV-TSX machines are re-packaged and returned to Division of Elections officials.
8. The functional test checklist documents are collected and scanned for historical purposes. Backed up electronic storage should be used to maintain the integrity of the functional checklist documentation.

A functional check of the Voter Card Encoder devices is recommended prior to each election. A complete history of the Voter Card Encoder functional testing is not recommended at this time.

GEMS functional testing is recommended on a per election basis and it is further recommended that the test documentation be archived in manner similar to that suggested for the AV-OS and AV-TSX machines. A sample GEMS functional test lifecycle is presented below.

1. Election cycle checklist is generated for each election system GEMS.
2. Functional testing is performed on each GEMS machine prior to the administration of the election.
3. The functional test checklist is completed by the test technician and is returned to the appropriate individual for historical archiving. Any anomalies or inconsistencies are noted in the functional test checklist form and are thus permanently recorded.

3.2 AccuVote Formatting and Clearing Procedure

The AccuVote system stores election ballots and vote tabulation data on a variety of different media during the process of an election. It is desirable from a security standpoint to clear and re-format the electronic storage media prior to use during each election cycle. Two different Election Management models were developed by Premier Election Solutions in response to the State of California de-certifying the Diebold equipment for use in California. It is recommended that the Division of Elections implement the Air Gap Election Management model as presented in Premier Elections Solutions document Plan on Formatting and Clearing Program Storage on Voting System, Revision 1.0 (2007).

3.2.2 GEMS Server Configuration

The Air Gap election management model requires the use of three separate host computers and maintains integrity and security by limiting the operations performed on each computer platform. The purpose of each computer is summarized below.

GEMS Server 1: GEMS server 1 is used to create election definitions, ballot templates and to download data to the voting machine memory cards.

GEMS Server 2: GEMS server 2 is used to capture uploaded election results from the AV-TSX and AV-OS precinct machines.

Workstation Computer: The workstation computer (more than one is possible) is used to clear the contents of AV-TSX memory cards prior to re-use in the AccuVote election system. The workstations used for this purpose should be dedicated to memory card storage clearing and should be minimally configured.

See Section 3.2 of Plan on Formatting and Clearing Program Storage on Voting System, Revision 1.0 (2007) for more information

3.2.3 AV-TSX PCMCIA Memory Card Storage Clearing

The contents of the AV-TSX memory cards should be cleared prior to each election cycle. The workstation computer(s) should be used to reformat the contents of each PCMCIA memory card. See Section 4.4 of Plan on Formatting and Clearing Program Storage on Voting System, Revision 1.0 (2007)

3.2.4 AV-OS Memory Card Storage Clearing

The contents of the AV-OS memory cards should be cleared using an AV-OS machine prior to each election cycle. See Section 4.5 of Plan on Formatting and Clearing Program Storage on Voting System, Revision 1.0 (2007) for details on the AV-OS memory card clearing procedure.

3.3 AV-OS Regional Center Tests

In addition to the existing functional tests specified by the Division of Elections (see Sections 1.1 and 1.2), the following additional tests and / or actions are recommended for each election cycle.

The majority of the tests or actions listed below require Diagnostics Mode access to the AV-OS machine.

3.3.1 Key Functionality Check

Locate all AV-OS keys. The AV-OS system utilizes a key for printer access and a key for ballot box access. Verify that AV-OS printer key opens printer door. Verify that ballot box key opens security plate and all other ballot box access points to ensure key functionality.

3.3.2 Serial Number Recording

Record the hardware serial number of the AV-OS machine in the functional checklist document. This procedure ensures that the documentation associated with the test is associated with a specific AV-OS machine and traceability of the machine's life can be

maintained. The State of Alaska asset tag should also be recorded if it is present. The asset tag should not be used in lieu of the serial number but in addition to it.

3.3.3 Firmware Version Validation and Recording

Record the firmware version of the AV-OS machine. Validate the reported firmware version against the known correct version. Do not use AV-OS if reported firmware version does not match expected value.

3.3.4 System Clock Setting

Verify that the system clock is set. If the clock is not set properly follow the procedure in the AccuVote-OS user's guide to set the clock. The clock maintains the date and time in the AV-OS machine and is backed up by the system battery (Diebold Election Systems AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.2, 2005).

3.3.5 LCD Test

This test confirms that the AV-OS machine's LCD display can properly reproduce all of the required text characters (AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.4, 2005).

3.3.6 System Memory Test

This test writes a set of test data to the AV-OS system memory and reads it back from the system memory. This test is successful if the data read is identical to the data written to system memory (AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.5, 2005).

3.3.7 Memory Card Test – REQUIRES A BLANK AV-OS MEMORY CARD

This test writes a set of test data to the AV-OS memory card and reads it back from the memory card. This test is successful if the data read is identical to the data written to the memory card (AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.6, 2005).

3.3.8 Printer Test

This test is executed during the Memory Card Test and validates the printer functionality by printing a subset of the standard character set on the printer tape (AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.6, 2005).

3.3.9 Auxiliary Serial Port Test

This test confirms that the modem interface is functional to ensure that election results can be properly transmitted upon election close. This is an internal test and does not require a connection to the Public Switched Telephone Network (AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.8, 2005).

3.3.10 Card Reader Test

This test confirms that the optical scanning read sensor channels (34 total on each ballot side) are functioning properly. It is not recommended to perform the card reader test using the "RECIRCULATE BALLOTS?" mode.

3.4 AV-OS Precinct Tests

The precinct testing involves a subset of the Regional Center level testing. The purpose of the precinct level testing is to confirm that the machine is not physically damaged and to detect high level problems with the AV-OS machine.

1. Physical Damage Inspection (see Section 2.1.1)
2. Serial Number Recording (see Section 3.2.2)
3. Firmware Version Validation and Recording. (see Section 3.2.3)
4. Key Functionality Check (see Section 3.2.1)

3.5 AV-TSX Regional Center Tests

The following tests are recommended to be performed at the regional center before an AV-TSX voting machine is distributed to a precinct for use in an election.

3.5.1 Physical Damage Inspection

The AV-TSX machine is inspected for physical damage during shipment or setup. All tamper-evident seals are checked to confirm that the AV-TSX machine has not been compromised. The security hologram is inspected during the physical damage inspection.

3.5.2 Machine Serial Number Validation

The AV-TSX hardware serial number is recorded on the checklist functional test sheet. Once the machine has booted, access the software reported serial number from the settings menu and confirm that the physical serial number and the software serial number match (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.1.1, 2005)

3.5.3 Hardware and Firmware Version Validation

The AV-TSX Bootloader version, Windows CE version and BallotStation versions are checked and recorded during AV-TSX system boot after power is applied to the machine.

3.5.4 Card Reader Port Validation

This test confirms that the smart card reader can perform the required read / write operations without error (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.1.2, 2005).

3.5.5 Date and Time Programming

This procedure sets the date and time in the AV-TSX machine (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.2, 2005).

3.5.6 Screen Display Calibration

This procedure calibrates the touchscreen and ensures that voter selections match with the software display presented to the user (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.3.2, 2005).

3.5.7 Printer Test

This test ensures that the AV-TSX VVPAT printer can printer the required paper ballot without error (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.4.1, 2005).

3.5.8 Audio Test

This test ensures that the audio output subsystem of the AV-TSX machine is operational (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.7, 2005).

3.5.9 Modem Test

This test validates the AV-TSX internal modem functionality and confirms the AV-TSX's ability to send data to the internal modem (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.9, 2005).

3.5.10 Security Setting Validation

This procedure validates the security settings of the AV-TSX for use in the election. The security setting validation procedure should include certificate validation and key signature validation. It may be desirable to implement the Key Card Tool key update procedure during this functional test step (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.10, 2005)

3.5.11 Central Administrator / Supervisor Access Test

A valid central administrator card and a valid supervisor card should be inserted into the AV-TSX machine following the Key Card update to ensure that central administrator access is available. An invalid central administrator and an invalid supervisor card should be inserted into the AV-TSX machine following the Key Card update to ensure that the security keys are properly transferred and the AV-TSX machine has been secured.

3.6 AV-TSX Precinct Tests

The precinct level tests for use with the AV-TSX are a subset of the regional center tests. The recommended suite of precinct tests is given below.

3.6.1 Physical Damage Inspection (see Section 3.4.1)
3.6.2 Machine Serial Number Validation (see Section 3.4.2)
3.6.3 Hardware and Firmware Version Validation (see Section 3.4.3)
3.6.4 Printer Test (see Section 3.4.7)
3.6.5 Supervisor Access Test (see Section 3.4.11)

3.7 Voter Card Encoder Tests

The Voter Card Encoder is used to create valid voter cards for use in the AV-TSX machines. Each Voter Card Encoder device should be tested prior to use in a precinct for voting during an election.

3.7.1 Voter Card Encoder Physical Damage Check

Inspect the Voter Card Encoder for visible physical damage.

3.7.2 Voter Card Encoder Display Check

The Voter Card Encoder should be powered on and the display should be checked to ensure that it is visible and all characters are visible. Fading should not be evident on the LCD display.

3.7.3 Voter Card Encoder Firmware Check

This procedure checks the Voter Card Encoder firmware level and ensures that the proper revision of firmware is present on the Voter Card Encoder.

3.7.4 Voter Card Encoder Supervisor Access Check

Supervisor access to the Voter Card Encoder should be verified.

3.8 GEMS Server / Workstation Tests

The AccuVote GEMS server is used to create election definitions, ballot templates and to download data to the voting machine memory cards as well as to receive uploaded precinct results from AV-TSX and AV-OS machines. Use of the Air Gap Election Management model (see Section 3.2) requires implementing two GEMS servers for each election. Both GEMS servers should have functional tests performed prior to use during an election cycle. A third workstation is used to wipe AV-TSX memory cards prior to election programming.

3.8.1 GEMS BIOS (Built-in Operating System) Password Validation

The GEMS server should implement a BIOS password policy compliant with the password management plan (Appendix E – Physical Password Management Recommendations, 2008).

3.8.2 Verify System, Service Pack, Server Model, Processor, Disk Size and RAM Parameters

The GEMS server should have the system parameters listed above checked prior to use to ensure that tampering has not occurred on the system.

3.8.3 GEMS Software Hash Verification

The GEMS.exe application should be validated by calculating both MD5 (Message-Digest 5) and SHA (Secure Hash Algorithm) hash functions. These hash codes should be compared with those registered with the National Software Reference Library (http://www.nrsl.nist.gov/votedata.html). Known vulnerabilities exist with the MD5 hash function and as a result both the MD5 and SHA hash functions should be calculated (Premier's Windows Configuration Guide, Revision 3.0, Section 10, 2007).

3.8.4 Loaded Software Confirmation

The GEMS server should be checked to ensure that only Winzip v11, Adobe Acrobat 8, Adobe Audition 2.0 or Sony SoundForge 8 and Nero Burning ROM 8 are the only applications loaded on the server.

3.8.4.1 GEMS Operating System Update Packages Validation

The GEMS server should have the recommended operating system update packages installed (Premier's Windows Configuration Guide, Revision 3.0 Section 4, 2007).

3.8.4.2 GEMS Operating System Services Validation

The GEMS server should have the recommended services running (Premier's Windows Configuration Guide, Revision 3.0 Section 5, 2007). All other system services should be disabled.

3.8.4.3 GEMS Operating System Data Execution Protection Module Validation

The GEMS server should have the Data Execution Protection (DEP) modules turned on as indicated in Premier's Windows Configuration Guide, Revision 3.0, Section 6 (2007).

3.8.4.4 GEMS Operating System Security Policy Validation

The GEMS server should have security policies validated which are in compliance with the SOAESP recommended password policy and which are compliant with Premier's Windows Configuration Guide, Revision 3.0, Section 7 (2007).

3.8.4.5 GEMS Server File Permission Validation

The GEMS server file permissions should be assigned as indicated in Premier's Windows Configuration Guide, Revision 3.0, Section 8 (2007).

3.8.4.6 GEMS Operating System Registry Permission Validation

The GEMS server registry permission should be assigned as indicated in Premier's Windows Configuration Guide, Revision 3.0, Section 9 (2007).

3.8.5 GEMS Server Date and Time Adjustment

The date and time on the GEMS server should be set to the current values prior to use during an election.

3.8.6 Network Address Validation

The network address reported by the GEMS server should be checked prior to use to ensure that it is NOT connected to a network.

3.8.7 GEMS Acceptance Test Database Test

The GEMS acceptance test database should be loaded and the contents of the test database validated using the GEMS software.

3.8.8 GEMS Database Backup

The GEMS database backup functionality should be confirmed prior to use of the GEMS software for election management. Ensure that a backed up database file can be properly read into the GEMS software.

3.8.9 GEMS Print Test

The GEMS printing functionality should be validated by initiating an “Administrative Report” from within the GEMS software. Both the hardware printer driver and the pdf printer driver should be tested.

3.8.10 Key Card Tool Test

A dedicated Key Card Tool workstation should be used to perform the Key Card Tool test. This workstation should be used to generate new security keys on a smart key card. The keys loaded on the smart key card should be confirmed by removing the card and then reading the keys back into the Key Card Tool software.

4 Recommendations

It is recommended that the Division of Elections implement all of the recommended tests presented in this document in addition to the tests already being used. The addition of the tests detailed in this document provides a more comprehensive functional check out of the system and reduces the potential problems encountered on election day. Adoption of the historical logging of checklist documentation ensures that the lifecycle of each voting machine is documented and available for review at a later time.

Appendix N - AccuVote Logic and Accuracy Guidelines

1 Introduction

The logic and accuracy guidelines presented here establish a minimum set of requirements to confirm that each electronic voting machine is producing reliable, accurate results.

This document is organized by first presenting the currently implemented logic and accuracy procedures in use by the Division of Elections. Following the currently implemented procedures a set of additional recommendations is presented which is intended to enhance the output of the logic and accuracy testing.

2 Current Logic and Accuracy Procedures

2.1 AccuVote Optical Scan (AV-OS)

The AV-OS machines are tested for logic and accuracy using a test deck of ballots with known results. The logic and accuracy test is implemented by shuffling the test ballot deck to create a randomly oriented set of ballots. The user then verifies that the number of ballots fed into the AV-OS machine matches that reported on the AV-OS public LCD. The results of the test deck are printed in short form. The results printed on the AV-OS results tape are compared with the known outcome.

The AV-OS machine's memory card is then prepared for the election and the machine is powered off until the actual election is conducted.

2.2 AV-TSX

The AV-TSX are tested for logic and accuracy by following a procedure designed to identify election programming errors. This procedure first clears results that are already present on the memory card. The technician then prints a zero totals report to ensure that the results memory register of the memory card was cleared.

Once the memory card results register is cleared the technician then creates a voter access card for each ballot type being tested. Manual test mode is used (requiring voter access cards) to perform the logic and accuracy testing for each ballot type in the election. Once all of the ballot types have been voted the results are printed and reviewed to ensure that the voted values match the expected results. Once the logic and accuracy of the printed results is review the memory card is set to election mode and is physically removed from the AV-TSX machine.

2.3 GEMS

Currently no explicit logic and accuracy testing is performed by the Division of Elections.

3 Recommended Logic and Accuracy Procedures

3.1 AV-OS

The AV-OS logic and accuracy testing procedure presented here ensures that the logic of the ballot programming is correct and that votes cast in each oval position are accurately tabulated.

In order to perform the AV-OS logic and accuracy tests several sets of test ballots must be prepared corresponding to each ballot type to be used in the election. The following sections describe the three different test decks to be used for AV-OS logic and accuracy testing.

3.1.1 LAn Test Deck Test

The LAn (Logic and Accuracy for n candidates) test deck test validates that all candidates in all races and on all ballots are counted correctly. In the LAn test a test ballot is created for each possible contest where the voting outcome is produced as shown below (where n = 5):

Race 1 Test Deck	
Candidate	**Vote Count**
A1	1
B1	2
C1	3
D1	4
E1	5

Ballot 1	
Candidate	**Vote**
A1	X
B1	
C1	
D1	
E1	

Ballot 2	
Candidate	**Vote**
A1	
B1	X
C1	
D1	
E1	

Race 2 Test Deck	
Candidate	**Vote Count**
A2	1
B2	2
C2	3
D2	4
E2	5

Ballot 3	
Candidate	**Vote**
A1	
B1	X
C1	
D1	
E1	

Ballot 4	
Candidate	**Vote**
A1	
B1	
C1	X
D1	
E1	

The race tabulations above show the number of tabulated votes for Races 1 and 2. The sample ballots shown are the first four ballots in the test deck for race 1. A total of 15 ballots would be required for each race shown.

A test ballot deck should be produced for all races for each ballot style.

3.1.3 Multi-vote Test Deck

The multi-vote test deck is used for ballots where “vote for more than one” races are programmed. In these races the ballots should be filled out as follows.

3.1.3.1 Overvote Ballot

The overvote ballot contains one more oval on each “vote for more than one” race than is allowed by the election program. The sample ballot shown is for a “Vote for Three” race where 4 ovals were selected.

Overvote Ballot	
Candidate	**Vote**
A	X
B	X
C	X
D	X
E	

3.1.3.2 Test Ballots

The test ballot deck for the multi-vote case consists of ballot as shown below (Vote for 3 ballot with 5 candidates):

Multi-vote Ballot 1	
Candidate	**Vote**
A	X
B	X
C	X
D	
E	

Multi-vote Ballot 2	
Candidate	**Vote**
A	
B	X
C	X
D	X
E	

Multi-vote Ballot 3	
Candidate	**Vote**
A	
B	
C	X
D	X
E	X

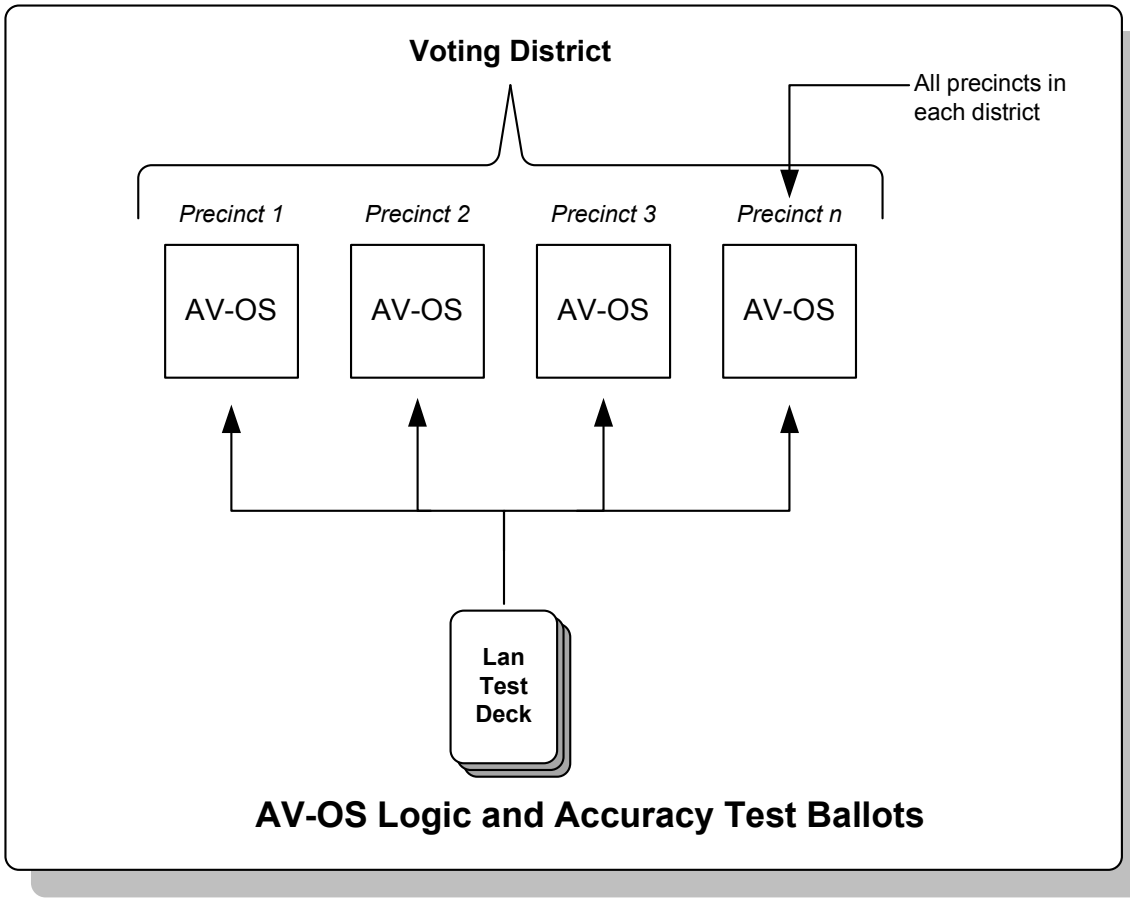
Multi-vote Test Deck	
Candidate	**Vote Count**
A	1
B	2
C	3
D	2
E	1

3.1.4 Logic and Accuracy Test Procedure

The logic and accuracy test should be performed on all AV-OS machines that will be used in the election. Following each test a precinct results tape should be printed and the results compared with the expected outcome. The results of the test should be uploaded to the GEMS and reports on the GEMS server should be generated which confirm the expected outcome.

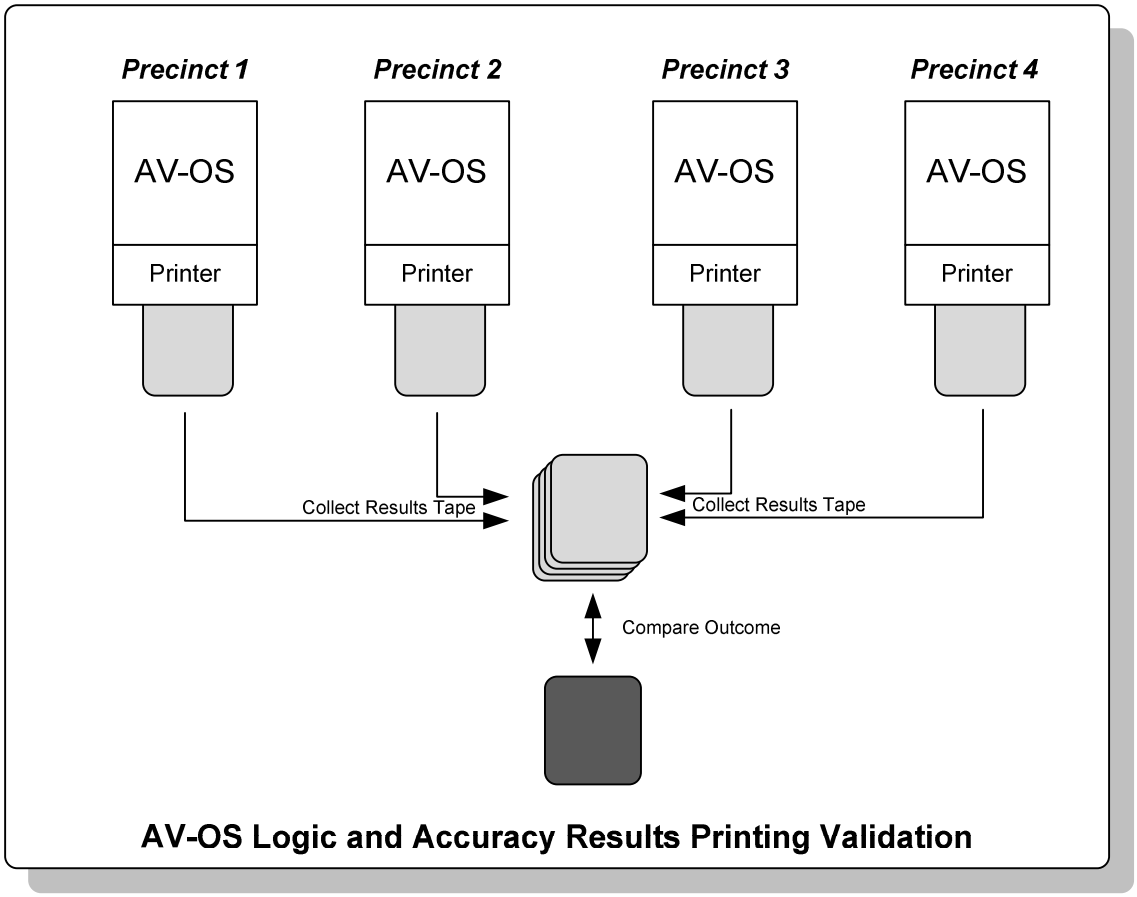
Logic and accuracy testing for the AV-OS system should be conducted by following the procedure below.

1. Run a LAn test deck through the AV-OS machine for every ballot style that will be used in the AV-OS machine.



LAn test ballots are run through every AV-OS in each voting district.

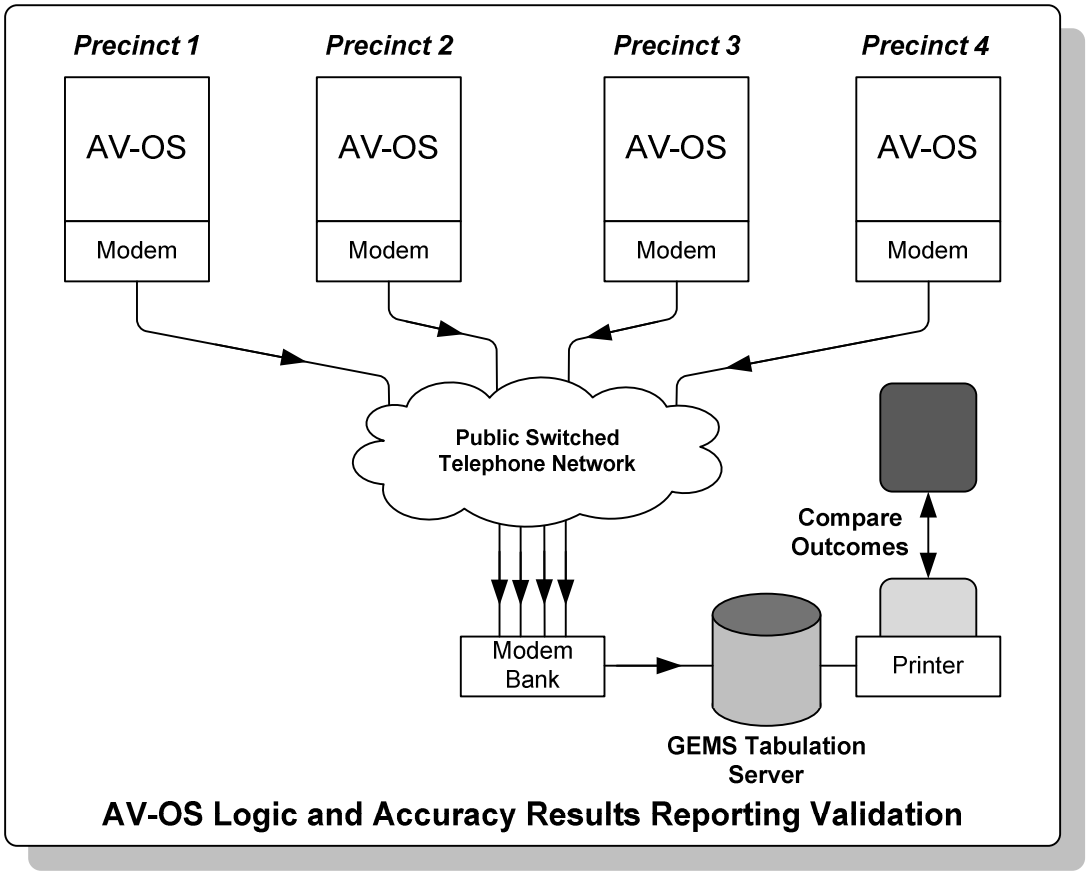
2. Print the results tape and confirm that the results match the expected value.



AV-OS Logic and Accuracy Results Printing Validation

Each AV-OS machine prints a results tape and these results tape outcomes are compared with the known expected outcome to ensure that tabulation is occurring accurately.

3. Transmit the results to the GEMS server.
4. Following the transmission of all results to the GEMS server a report is generated and the contents are compared with the expected value for the test ballot results.



5. The paper ballot decks generated for the use in the logic and accuracy tests as well as the logic and accuracy printed results should be archived together for historical purposes. Scanning of the results and electronic storage of these logic and accuracy test results is recommended.

3.2 AV-TSX

The AccuVote Touchscreen Ballot Station software offers the user two different approaches for logic and accuracy testing. These approaches are labeled Manual and Automated within the Ballot Station software.

3.2.1 Manual Logic and Accuracy Testing

In Manual Logic and Accuracy testing the user manually casts a series of test ballots to validate that the AV-TSX is properly counting ballots. The Premier recommended AV-TSX manual logic and accuracy test is performed by selecting the manual logic and accuracy test option within the Ballot Station software. The

manual test automatically casts a successively increasing number of ballots until the number of ballots is equal to the number of candidates in the largest race.

3.2.2 Automated Logic and Accuracy Testing

The AV-TSX Ballot Station software includes an option for automated logic and accuracy testing. In the automated test environment the tester selects a pre-determined combination of ballots to be voted. The system automatically casts the ballots and tabulates the results. The number of ballots cast is increased on each iteration until the number of ballots equals the number of candidates in the largest race on the ballot (as in the manual test mode). Additionally, a blank ballot is cast for each ballot set.

The tester can select from 5 different ballot testing options within the automated test mode. It is recommended that the test technician perform the Full Test by Ballot and the Full Test by Precinct automated tests.

The Ballot Station software offers two options while performing the automated test procedures. The *Use Ballot Rotation* option allows the user to rotate the candidate position. The *Provisional Ballots* option allows the user to specify the use of provisional ballots during the test.

3.2.2.1 Full Test by Ballot

The full test by ballot test votes a full set of ballots for every ballot on the memory card. Each unique ballot on the memory card is voted by casting votes as shown below.

AV-TSX Full Test by Ballot	
Candidate	**Vote Count**
A	1
B	2
C	3
D	4
E	5
Total Ballots	15

This procedure is iterated until all unique ballots on the memory card have been voted.

3.2.2.2 Full Test by Precinct

The full test by precinct test casts a full set of ballots for every base precinct present on the memory card. Ballots are cast in the same manner as shown in section 3.2.2.1 where the number of ballots cast is increased on each iteration until the number of ballots cast is equal to the largest number of candidates in that race.

3.2.3 Results Validation

3.2.3.1 Print Results

Once the logic and accuracy tests are completed it is recommended that the results be printed and the results on the printed tape be validated against the expected results.

3.2.3.2 Upload Results

The results of the logic and accuracy test should be uploaded to the GEMS server using the internal modem. Once the results have been uploaded an election report should be printed and validated against the expected results.

3.3 GEMS

3.3.1 Tabulation Accuracy Validation

The GEMS host computer in the Director's office in Juneau is used to tabulate logic and accuracy results transmitted during the logic and accuracy testing of each machine. The GEMS Summary, Statement of Votes Cast and the Cards Cast report results must be reconciled with the results obtained in the AV-OS and AV-TSX machines (GEMS 1.18 Election Administrator's Guide, 2006).

4. Recommendations

We recommend that the Division of Elections implement all of the tests presented in this document in addition to the tests already in use. The increased scope of the tests detailed here provides a more comprehensive validation of the logic and accuracy of the programmed election. Detailed documentation of the test results for each AV-OS and AV-TSX machine is recommended for each election cycle. Historical logging of these results is also recommended in electronic format.

Appendix O - AccuVote Touchscreen

Smart Key Card Enhancement Options

1. System Description

The AccutVote Touchscreen voting system is comprised of several different components. System security is maintained by utilizing a suite of smart cards to secure the election ballot, vote tallies, the touchscreen voting machine operating system, and other sensitive system data. The smart card system is comprised of four different smart cards, the Key Card Tool application and a smart card programmer.

This section describes each system component in the context of the key card tool application. Each component is described along with its interaction with the key card security implementation.

Key Card Tool Software

Key Card Tool is a software application created by Premier Election Systems for use with the AccuVote Touchscreen (AV-TSX) system. The Key Card Tool application allows users to create authentication keys and passwords on a personal computer platform and to write those authentication keys to smart cards for use in the touchscreen voting system.

Key Card Tool requires a personal computer workstation on which the Key Card Tool application runs as well as a smart card reader which interfaces to the personal computer communications port. The smart card reader is used to read and write authentication keys and passwords to individual smart cards.

Smart Key Card

The smart key card is the basis of the touchscreen system access security. The smart key card stores two authentication keys and two passwords. The smart card key is used to authenticate user access at the central administrator, supervisor and voter levels. The smart card key validates the user's authentication key against the key present in the hardware device being accessed. The data key is used to encrypt individual data files within the ballot station (firmware that operates on the touchscreen terminal). A password is stored to secure central administrator access and another is stored to secure supervisor access to the touchscreen machine.

The smart key card is programmed by Premier with default values for the security and data keys as well as the central administrator and supervisor passwords. These passwords are well known in the public domain and are considered insecure. Replacement of the key and password values is accomplished through the use of the Key Card Tool application.

The Key Card Tool application allows the user to select new values for the security key, data key, central administrator password, and supervisor password and to write these values onto a blank smart card.

Once the central administrator and supervisor smart cards have been updated with new keys and passwords these cards cannot be further updated without the use of the Key Card Tool application and the original security keys.

After the smart key card has been programmed with the values selected by the election officials, the card is removed from the programming device and must be used to update the authentication keys on the touchscreen devices and the voter card encoder devices.

Central Administrator and Supervisor Cards

The central administrator and supervisor cards are used to secure central administrator and supervisor access to the AccuVote Touchscreen machine. Central administrator access allows users an expanded set of system options within the AccuVote Touchscreen system not available to users with supervisor or voter access. Supervisor access allows election administrators to open and close elections, print paper records and to transmit election results to the GEMS.

Central administrator and supervisor cards must be updated using the Key Card Tool application at any time the keys and passwords are changed. The cards are updated by inserting the smart card into the card encoding device and following the software procedure after the smart key card has been created.

Central administrator and supervisor touchscreen device access is obtained by inserting the central administrator or supervisor card into the touchscreen device and entering the appropriate password. Upon insertion of the smart card the card security key is authenticated against the terminal key and the user is granted the appropriate level of access. A central administrator or supervisor card that does not have valid security and data keys will be rejected by the system. After 7 unsuccessful attempts at system access using a smart card with invalid keys the smart card will be permanently disabled.

Voter Access Card

The voter access card is used to allow voters to cast their votes on the electronically defined ballot. The voter access card is programmed by a voter card encoder that is under the authority of election administrators. The voter card encoder must be updated with the security and data keys when the key and password values are updated. Voter cards are not required to be programmed by the Key Card Tool application.

During an election after election officials determine that a voter is allowed to cast a ballot the vote card encoder is used to enable a voter card. The voting process of an individual voter proceeds as follows:

1. An election official creates a valid voter access card by inserting a default voter access card into the voter card encoder.
2. The voter takes the valid voter access card to a touchscreen terminal and inserts it into the smart card slot. The system authenticates the voter access card against the authentication keys present in the AccuVote system software.
3. The voter casts a ballot and completes the voting process.

4. The AccuVote system software overwrites the voter access card authentication keys with default values defined by Premier.
5. The voter removes the voter access card and returns it to an election official.
6. The process is restarted using the voter access card with default security key values.

Voter access cards with previously assigned or invalid authentication keys cannot be used to cast a ballot on a terminal containing authentication keys which do not match the smart card keys.

2. Logistical Impact

Implementing the security enhancements available through the Premier Election Systems Key Card Tool product requires the State of Alaska Division of Elections to modify the manner in which it transports and stores the AccuVote Touchscreen devices.

Every authentication key and password change requires a system-wide AccuVote Touchscreen firmware authentication key update. This update includes:

1. Smart Key Card
2. Central Administrator Cards
3. Supervisor Cards
4. Voter Card Encoder
5. AccuVote Touchscreen Terminal

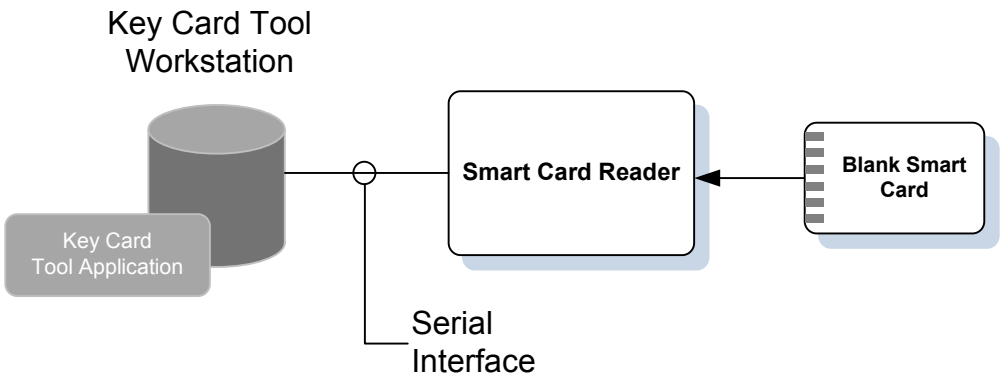
The system functions only when all hardware and software have the same authentication keys loaded.

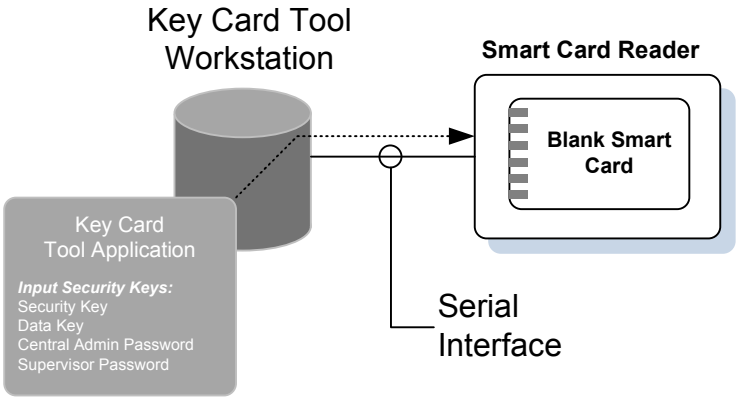
Currently the Division of Elections will ship AccuVote Touchscreen devices to remote communities for Primary elections. Upon completion of the Primary election the touchscreen terminals will remain in many remote communities until the general election some time later. This makes authentication key / password changes impossible during the “sleepover” period.

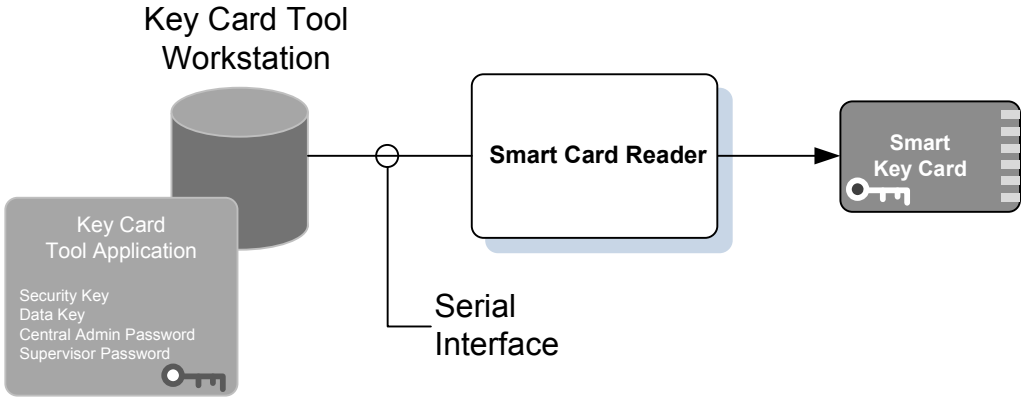
Implementing the highest level of security improvement in which the authentication keys / passwords are changed following each and every election requires the field equipment (touchscreen terminals and voter card encoders) to be returned to a central location for programming after the close of each election.

3. Recommendations

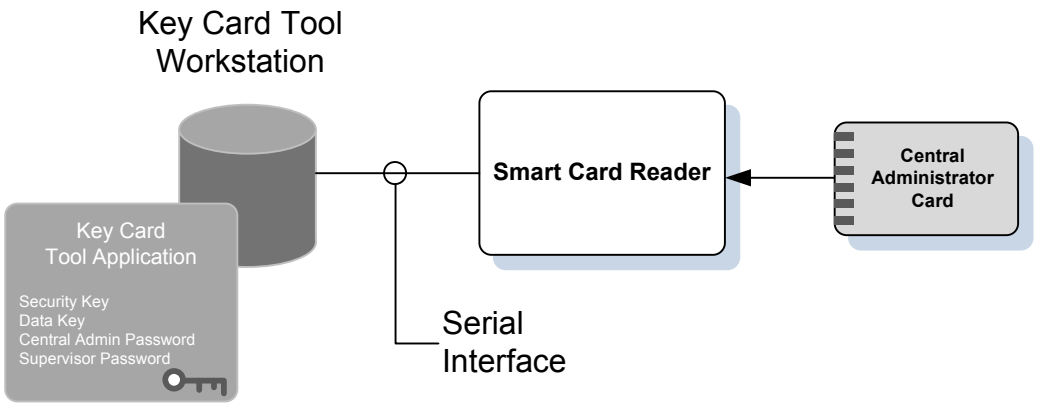
We recommend that the Division of Elections procure and implement the Key Card Tool application for use in the 2008 election cycle. We do not recommend returning the AV-TSX machines to have the encryption keys and passwords changed between the primary and general elections because of the significant logistical impact this would have on the Division of Elections. The use of the Key Card Tool application for each election cycle increases the security of the AccuVote Touch Screen system significantly.

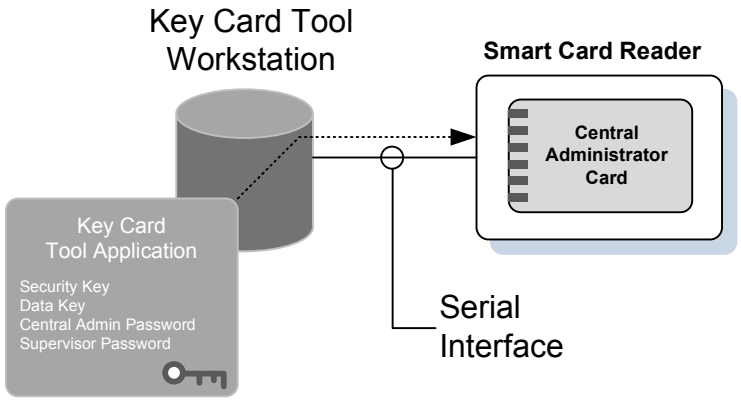


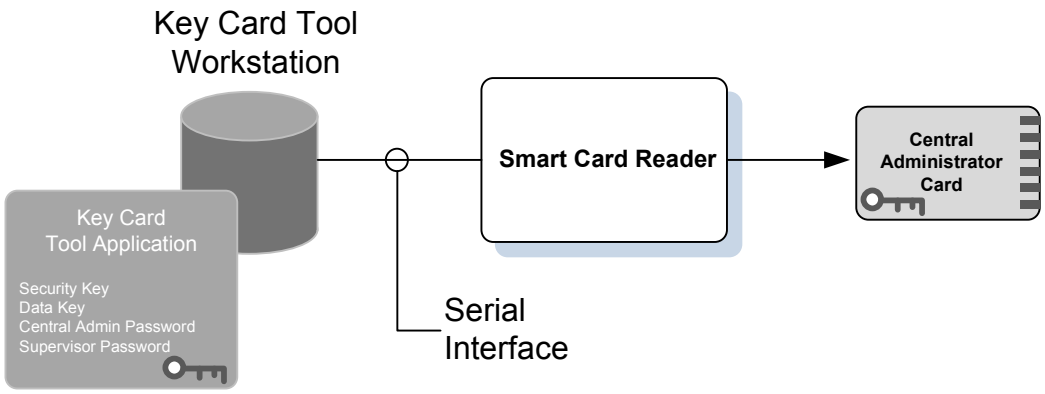




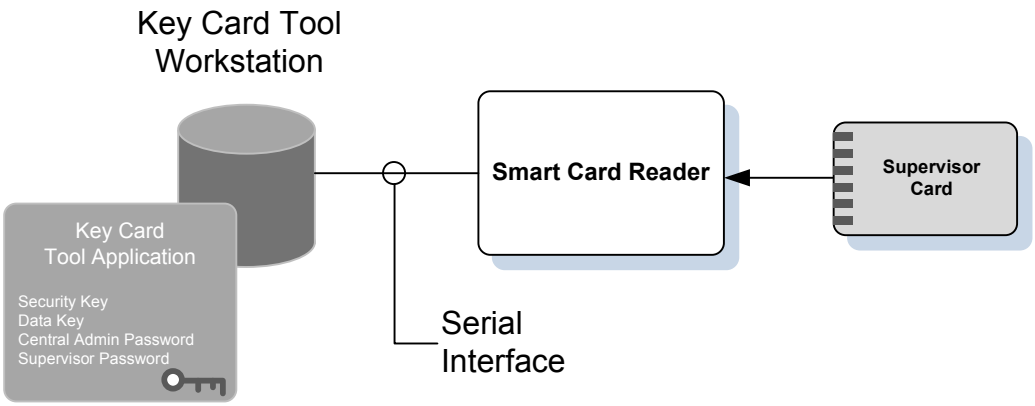
Premier Key Card Tool System Description			
Name:	Figure 1: Security Key Card Progamming		
Drawn By:	Mark Ayers	Date:	4/15/2008
Edited By:		Edited:	
Scale:	NTS	Sheet:	1 of 6

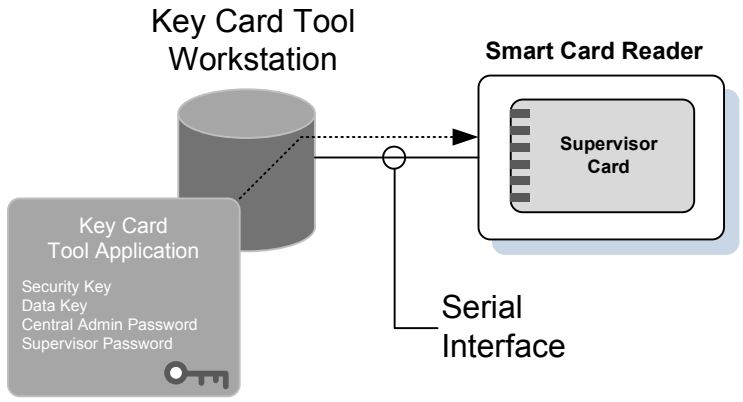


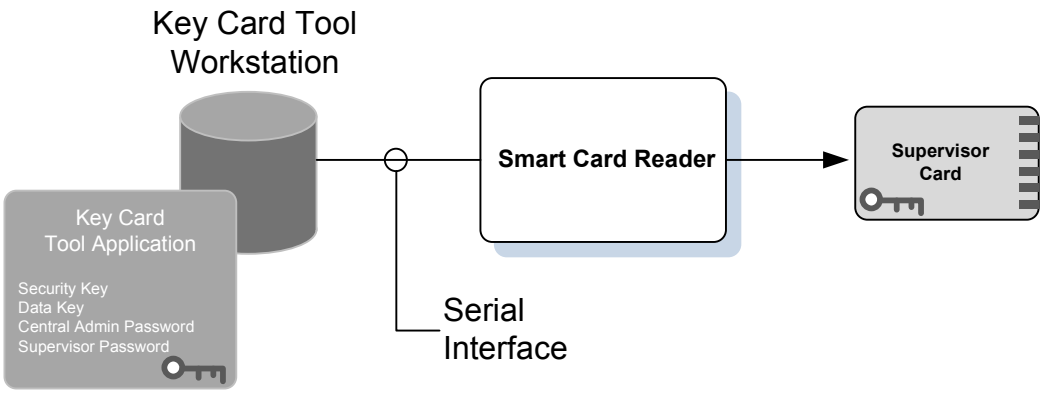




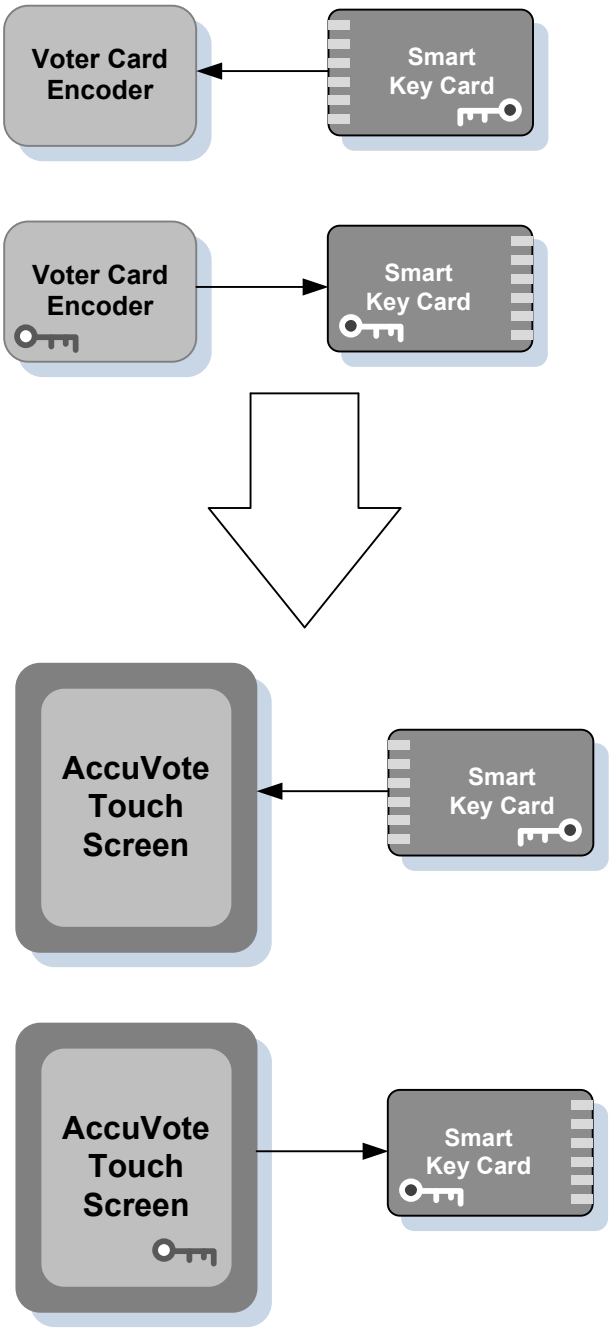
Premier Key Card Tool System Description			
Name:	Figure 2: Central Admin Card Programming		
Drawn By:	Mark Ayers	Date:	*4/15/2008*
Edited By:		Edited:	
Scale:	*NTS*	Sheet:	*2 of 6*



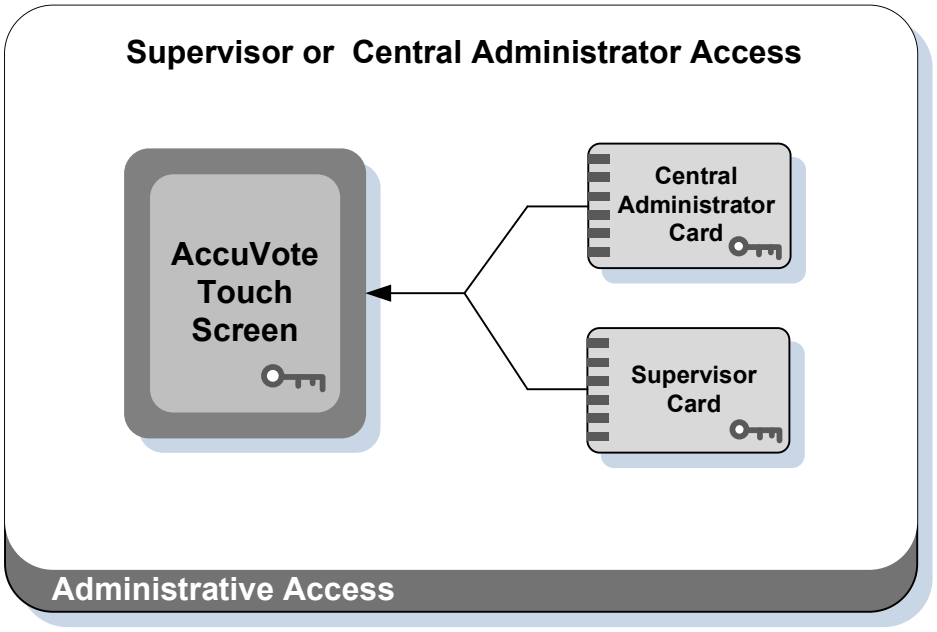


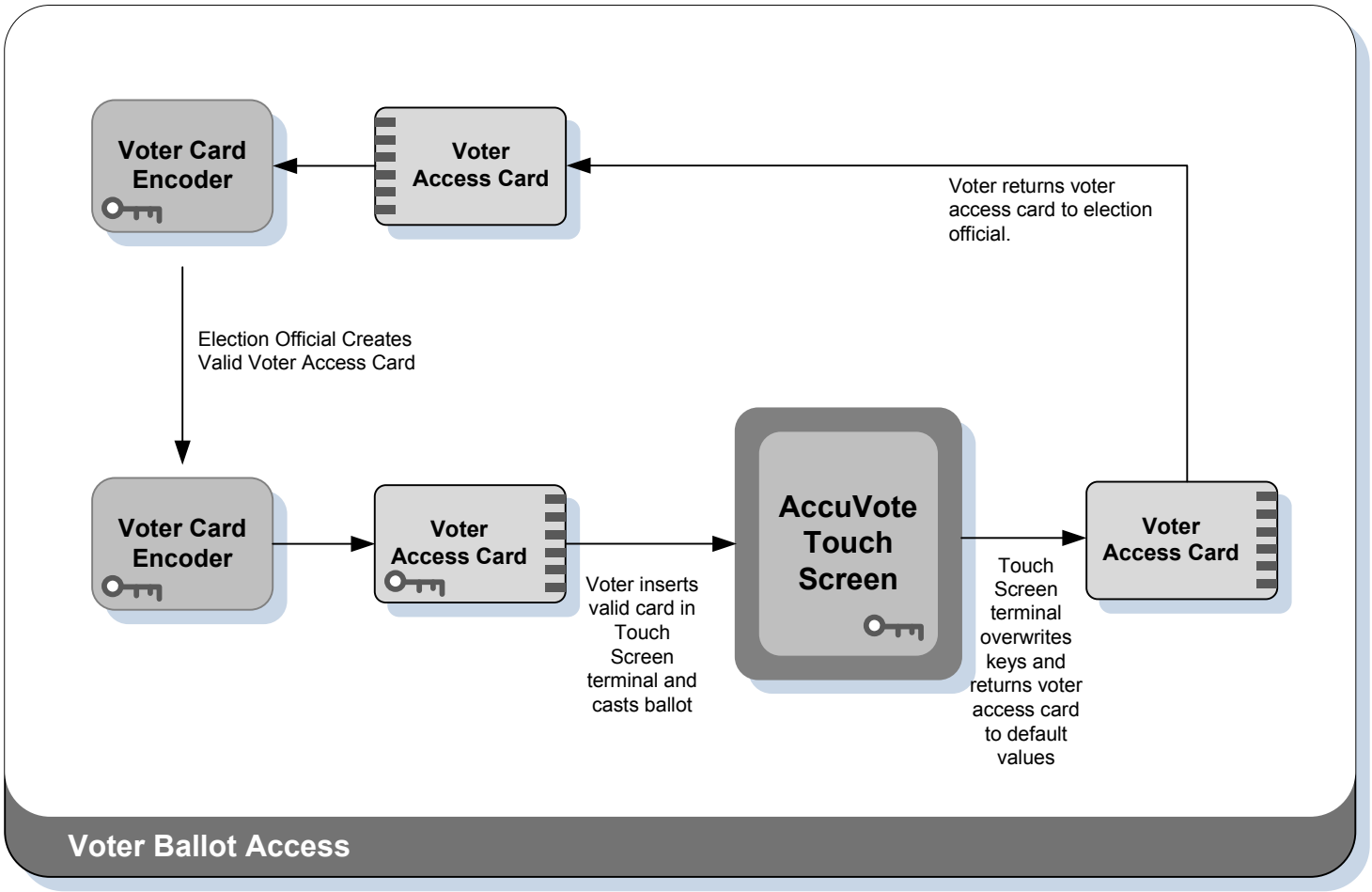


Premier Key Card Tool System Description			
Name:	Figure 3: Supervisor Card Programming		
Drawn By:	Mark Ayers	Date:	*4/15/2008*
Edited By:		Edited:	
Scale:	*NTS*	Sheet:	*3 of 6*

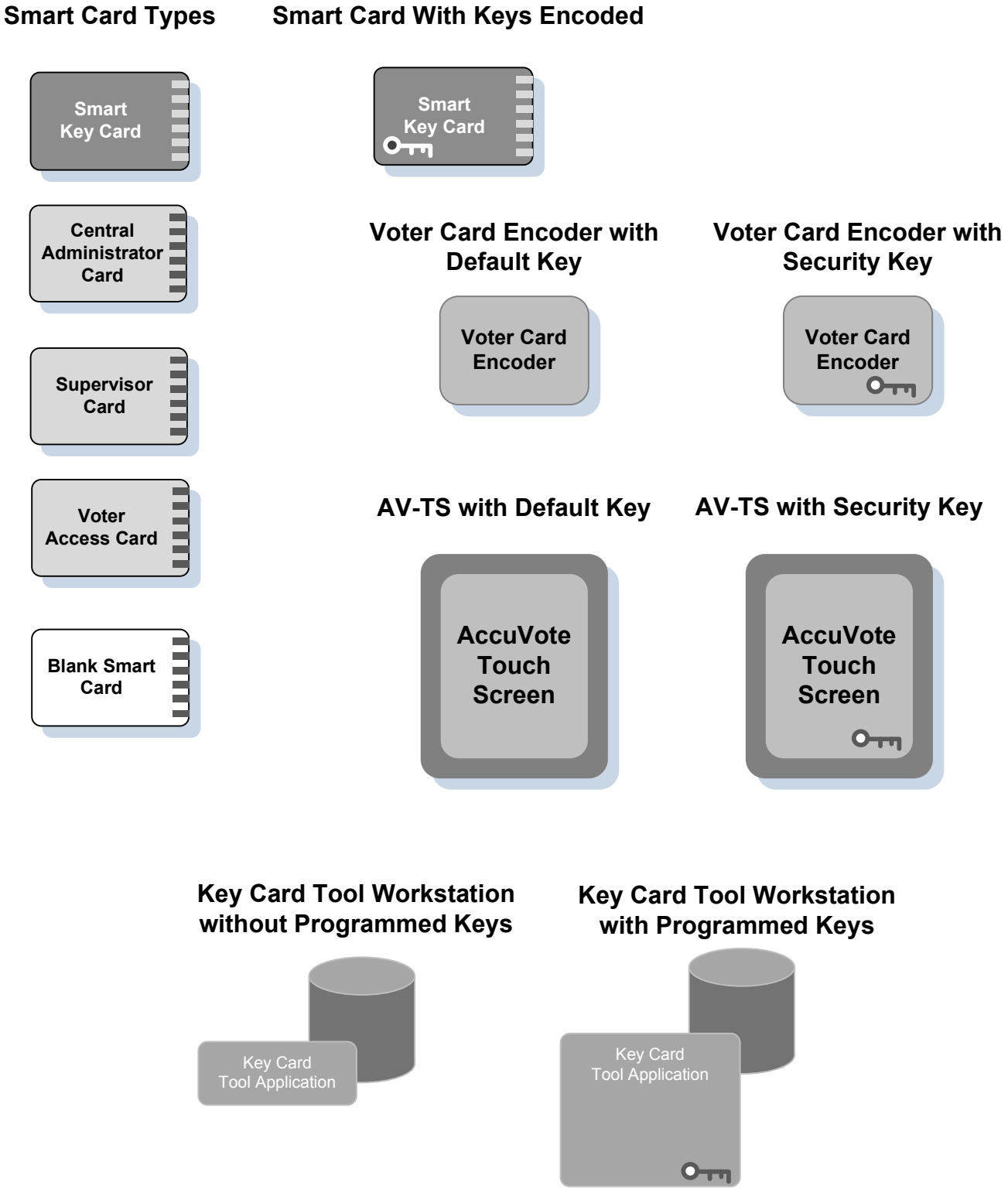


Premier Key Card Tool System Description			
Name:	Figure 4: Hardware Key Update		
Drawn By:	Mark Ayers	Date:	4/15/2008
Edited By:		Edited:	
Scale:	NTS	Sheet:	4 of 6





Premier Key Card Tool System Description			
Name:	Figure 5: Voting Process using Key Card		
Drawn By:	Mark Ayers	Date:	4/15/2008
Edited By:		Edited:	
Scale:	NTS	Sheet:	5 of 6



Premier Key Card Tool System Description			
Name:	Figure 6: System Overview Icon Legend		
Drawn By:	Mark Ayers	Date:	4/15/2008
Edited By:		Edited:	
Scale:	NTS	Sheet:	6 of 6

Appendix Q – Summary of Absentee Voting

Absentee Voting is a major component of the election process because, in the last election, 18% of the voters voted by absentee.

There are two broad categories of absentee voting. The first category includes **absentee** by (1.) mail, (2.) fax and (3.) special advanced requests. The second category is called **in person absentee** which includes (1.) special needs voting, (2.) early voting, and (3.) absentee in person.

The description of requirements is listed in the Division of Election web site. In all cases, the process starts with the request for ballots to be printed. This is done as part of the same order for ballots to the printer for the precinct voting 48 days before the election. The ballots are numbered in sequence with numbers of ballots printed from estimates based on previous elections.

Law requires that all absentee ballots be reviewed, opened and counted by the 15th day after the election. Absentee ballots are not part of the post-election audit process.

There is an **Absentee Voting Station Official Procedures** (Rev 5/2006) and a **Absentee Voting Official's Handbook** (Rev 4/25/06)

1. Absentee Ballots

Category 1 ballots are sent to the Division of Elections Absentee and Petition office in Anchorage by the printer.

1.1 Absentee by Mail

Deadline for by mail requests must be received 10 days before the election. Individuals can request either to vote for a single election or all elections in the calendar year. Voters receive their ballot by mail, complete it, and place the completed ballot into an included security sleeve. That is place that inside a return envelope, the envelope is signed and witnessed. The ballot envelope must be postmarked no later than Election Day. If mailed from within the United States, the envelope must be received within 10 days after Election Day. If mailed from outside the United States, it must be received within 15 days of Election Day.

The **by mail absentee** ballots are addressed to the respective Regional office. These envelopes are reviewed by the review board, opened and processed through an OS machines at the Regional office election evening. Either a separate machine is used or a OS machines that was used at the election, but with a separate memory card. Eligibility of absentee voters is accomplished with the Voter Registration Election Management System (VREMS). This system is completely separate from the GEMS system.

1.2 Absentee by Fax

GEMS generates the ballots **by fax** document as a PDF template that is distributed (faxed by computer) to those who requested the ballot by fax. Voters requesting this format can do so between 15 days before the election but no later that 5PM AST the day before Election Day. Voters have two options when receiving the ballot by fax. One is to return it **by fax** (to the Absentee and Petition Office) and the other is to **mail** it back to the respective Region Office. If faxed back, it must be received no later than 8 PM AST the day of the election. If mailed back, the ballot must be postmarked no later than the Election Day and received; within 10 days, if U.S postmarked or within 15 days if via international mail. Absentee voters are reminded that by returning their ballot by fax, means that they are voluntarily waiving their right to a secret ballot. Faxed ballots are sent from the Absentee and Petition office to the

respective Regional Office. The Region review board reviews each ballot for eligibility and determined if a full or partial count ballot. Ballots are placed in piles and two individuals together make a facsimile of the ballot for processing as an OS ballot.

1.3 Special Advance

This form of voting is available for individuals in remote Alaska or overseas who want an official ballot 60 – 32 days before the election. These requests result in the individual being sent both a special advance ballot and an official ballot to be voted absentee. If only the advanced ballot is returned to the Absentee office, it is entered into VREMS, and secured until 15 days after the election. The special advanced ballots are hand counted and the results manually loaded into GEMS. If the OS ballot is returned, it is entered into VREMS and forwarded to the respective Regional official. VREMS verifies if only the advanced ballot was received or if both the advanced ballot and the OS ballot were received. If both were received, the OS ballot is the only one that is counted. The Advanced ballots are accumulated to 15 days, then logged, reviewed by a review board and shipped to Juneau and entered officially in Juneau into GEMS.

2. In Person Absentee Voting

2.1 In person

Individuals may vote in person or through a representative up to 15 days prior to Election Day. Ballots are printed and delivered to the Regional offices. Each region has appointed absentee voting locations and distributes ballots to these locations. Some have house seat ballots for all 40 house seats and other absentee sites have only the ballots for the respective Regions' House Districts for that voting location. The Regional Offices (and Wasilla satellite are also absentee voting locations with ballots of all 40 representative districts and available for all 15 days.

Region	Number of Locations
I	30
II	11
III	20
IV	15

Some of the absentee voting locations are only available for Election Day or Election Day and the day before. The Official Election Pamphlets outline the locations and time that these locations are open for absentee voting.

2.2 Special Needs Voting

A qualified voter who is disabled may apply for an absentee ballot through a personal representative who can bring the ballot to the voter.
(following bullets taken from Division of Elections web site:
http://www.elections.alaska.gov/abinfo.php)

- A personal representative can be anyone over 18, except a candidate for office in the election, the voter's employer, an agent of the voter's employer, or an officer or agent of the voter's union.
- Ballots are available 15 days before the Primary, General or Statewide Special Election at any Regional Elections Office:

  - **Anchorage:** 2525 Gambell St, Ste 100 , 522-8683
  - **Fairbanks:** State Office Building, 675 7th Ave., 451-2835

- **Juneau:** Mendenhall Mall, 9109 Mendenhall Mall Road, Suite 3, 465-3021
- **Nome :** 103 E Front Street, 2nd Floor - State Office Building, 443-5285
- **Matanuska-Susitna :** 1700 E. Bogard Road, Building B, Suite 102 - North fork Professional Building, 373-8952

- Ballots are available 15 days before the Primary, General or Statewide Special Election from any Absentee Voting Official.
- Ballots are also available on Election Day from the voter's polling place, unless there is an Absentee Official in the area.
- The Personal Representative brings the completed application to an Election Official for a ballot and takes the ballot to the voter.
- The voter completes a certificate authorizing the Personal Representative to carry their ballot, votes the ballot privately, places it in a secrecy sleeve and seals it inside the envelope provided.
- The Personal Representative brings the voted ballot back to the Election Official by 8:00 p.m. on Election Day.

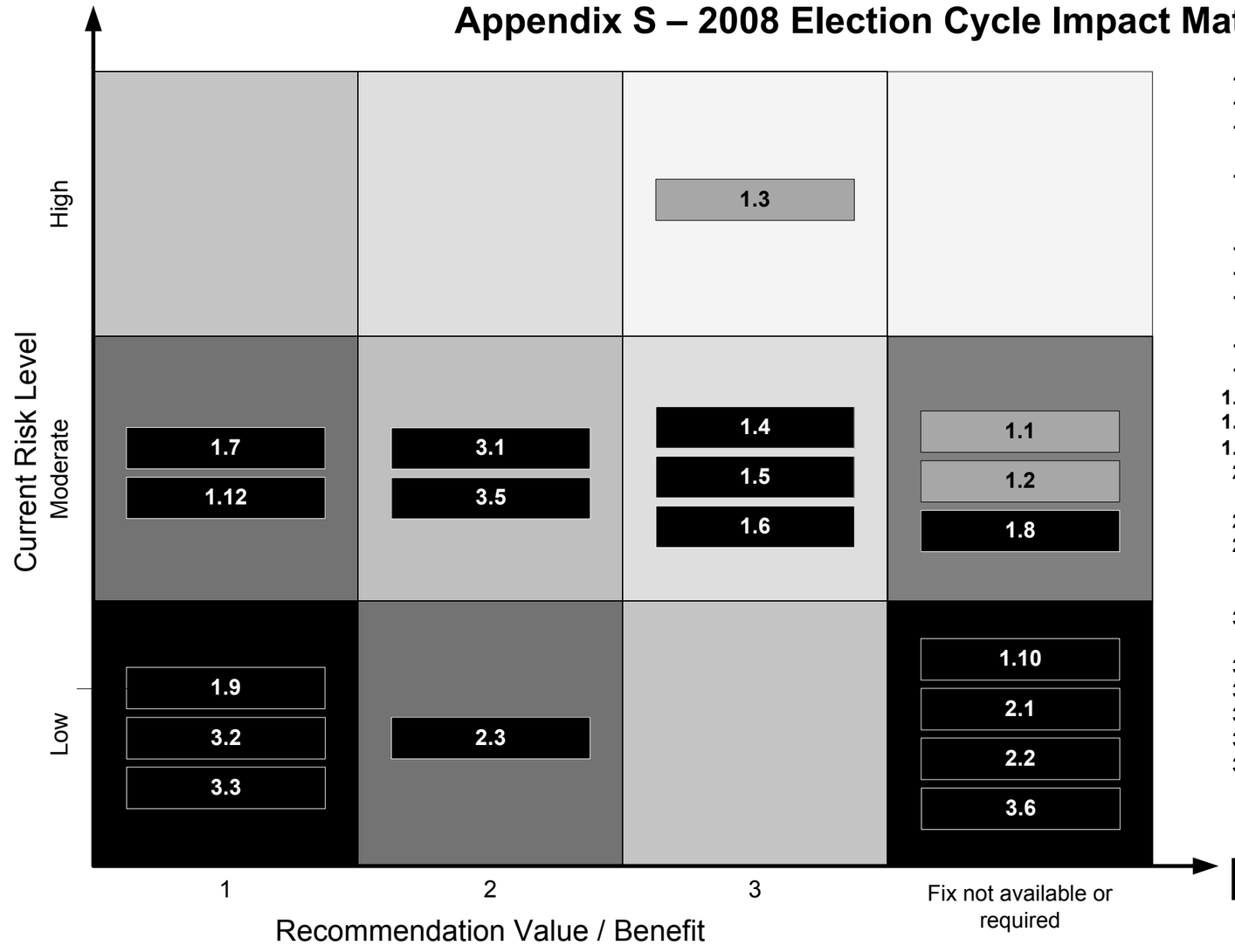
2.3 Early Voting In Person

These **early vote in person** ballots are only issued at the Regional offices (and Wasilla office). They are voted in the office and then sealed, placed in a separate ballot box. These ballots are opened and OS scanned election night with the ballots retuned to Juneau with the Regions election documents.

Appendix R – Master Matrix: Recommendations, Risk and Value Assessment

Document Section	Scope of Work Item	Current Risk Level (H, M, L)	Current Election Cycle Recommendation	Value / Benefit of implementing recommendation in the 2008 election cycle (3, 2, 1)	Residual Risk Level after implementation of 2008 election cycle recommendations (H, M, L)	Future Election Cycle Recommendation	Residual Risk remaining from 2008 election cycle (H, M, L)	Value / Benefit of implementing recommendation in the current election cycle (3, 2, 1)	Residual Risk Level after implementation of future election cycle recommendations (H, M, L)	Constraints / Notes
1.0	**Defense in Depth**									
1.1	Assure 1.2 Upgrade Cost Analysis	M	Maintain current revision of AccuVote software, perform cost benefit analysis to determine best resource utilization approach.	N/A	M	Upgrade to Assure 1.2 when certified	M	3	L	Funding and logistical planning of the upgrade represents a significant dedication of resources.
1.2	Assure 1.2 Functionality Upgrade Analysis	M	Maintain current revision of AccuVote software.	N/A	M	Upgrade to Assure 1.2 when certified	M	3	L	Certification of the Assure 1.2 software is required prior to installation.
1.3	Division of Elections Security Enhancements and Features Analysis	H	Implement selected recommendations from Appendix D - Division of Elections Enhancement Analysis. 2.1-2.5, 2.8, 2.10, 2.13, 2.16, 2.17, 2.18, 2.19, 2.23, 2.29	3	M	Implement remaining recommendations included in Appendix D.	M	3	L	Determination of which selected enhancements are implemented in the current election cycle requires input from the Division of Elections.
1.4	Implement procedures to minimize technology risks not addressed by existing or upgraded systems	M	Implement procedures described in other sections. Important to maintain many of the processes already in place.	3	L	Monitor research on election processes and implement changes, as appropriate.	L	2	L	Implementation of technology updates and changes is crucial to maintaining election system security and performance.
1.5	Password Management	M	Change passwords on all affected hardware as outlined in password management plan (Appendix E).	3	L	Develop password management procedures to implement password changes and tracking for future election cycles to ensure password policies are followed consistently.	L	2	L	Resources to develop password management procedures will likely not be available until after the 2008 election cycle.
1.6	Chain of Custody	M	Use tamper evident seals on AV-OS and AV-TSX machines.	3	L	Implement EPROM bar code identification and inventory management.	L	2	L	Bypass mail, rural home storage, poll worker training and uncertainty about tampering false alarms present challenges to implementing a robust tamper seal security plan.
1.7	Best practices for equipment storage between elections	M	Follow Chain of Custody recommendations. Purchase Division of Elections owned equipment for North Slope Borough. Safes are recommended for use in DoE offices to store keys and passwords.	1	L	Improve physical storage security such as room security, access alarm, etc.	L	3	L	Equipment storage outside of regional centers and hubs is not addressed by the recommendation. Security during transportation is a concern.
1.8	Trusted Personnel and single points of access	M	None	N/A	M	Require background checks on new employees with access to election equipment and confidential information	M	2	L	State and union regulations may limit the implementation of background checks. Access to proprietary information should be limited.
1.9	Redundancy	L	Two person inspection and sign off on tamper evident seals.	1	L	Add two-person sign-off to manual entry of election results and tamper seal inspections.	L	2	L	Poll worker resource constraints could make tamper seal inspections difficult on election day.
1.10	Paper Ballot tampering vulnerability	L	None	N/A	L	None	L	N/A	L	Maintain current paper ballot system.
1.11	Master Vulnerability Matrix	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
1.12	Security Training	M	Develop materials to train poll worker in election security.	1	L	Monitor new procedures and implement as appropriate.	L	1	L	Poll workers are temporary employees, usually retirees, many don't complete training, a lot of information to cover in training session, limits to poll worker authority.
2.0	**Fortification of Systems**									
2.1	Assess the integrity of the hardware and software of the electronic voting systems and their ability to accurately tabulate and report results.	L	Implement Key Card Tool application. Implement GEMS Air Gap Server model system. Implement dedicated AV-OS machine for programming AV-OS memory cards.	N/A	L	None	L	N/A	L	None
2.2	Preliminary Results Data Collection Assessment	L	None	N/A	L	None	L	N/A	L	None
2.3	Evaluate the reliability and accuracy of the optical scanning and touch screen systems in Alaska weather and transportation/handling conditions.	L	Implement new shipping containers for optical scanning systems (Pelican™. Products 1600 series or similar)	2	L	None	L	1	L	None
3.0	**Confidence in Outcomes**									
3.1	Procedures for functionality, logic and accuracy testing for systems and memory cards.	M	Implement increased test scope for functional, logic and accuracy testing.	2	L	Implement test results documentation and storage policies.	L	2	L	Storage of machine test results may require implementation of an electronic data storage system.
3.2	Methods to improve voter confidence	L	Increase voter use of AV-TSX machines to improve voter anonymity.	1	L	Monitor research on election processes and implement changes, as appropriate.	L	N/A	L	Changes to Alaska's audit procedure require legislative approval. DoE staff size limits is ability to develop new poll worker training and recruitment programs.
3.3	Metrics and continuous improvement	L	Implement a multi-year, multi-phase approach to improving election procedures and equipment.	1	L	Multi-year, multi-phase approach	L	2	L	A multi-year, multi-phase approach requires staff training and coordination between DOE departments.
3.4	Weekly email summary	N/A	Provide on-going summary	N/A	N/A	Provide on-going summary	N/A	N/A	N/A	
3.5	Absentee and questioned ballot process	M	Implement 2008 election cycle security improvements.	2	L	Same as current election recommendations.	L	2	L	The absentee ballot system is subject to the same vulnerabilities as the standard election system but the AV-OS machines are exposed for a 2 week period of time.
3.6	Random sampling methodologies	L	None. Current research is not conclusive enough to recommend a change to the DoE methodology.	N/A	L	Implement new sampling procedure as appropriate and approved by statute.	Unknown	Unknown	Unknown	Changes must be approved by statute

Appendix S – 2008 Election Cycle Impact Matrix

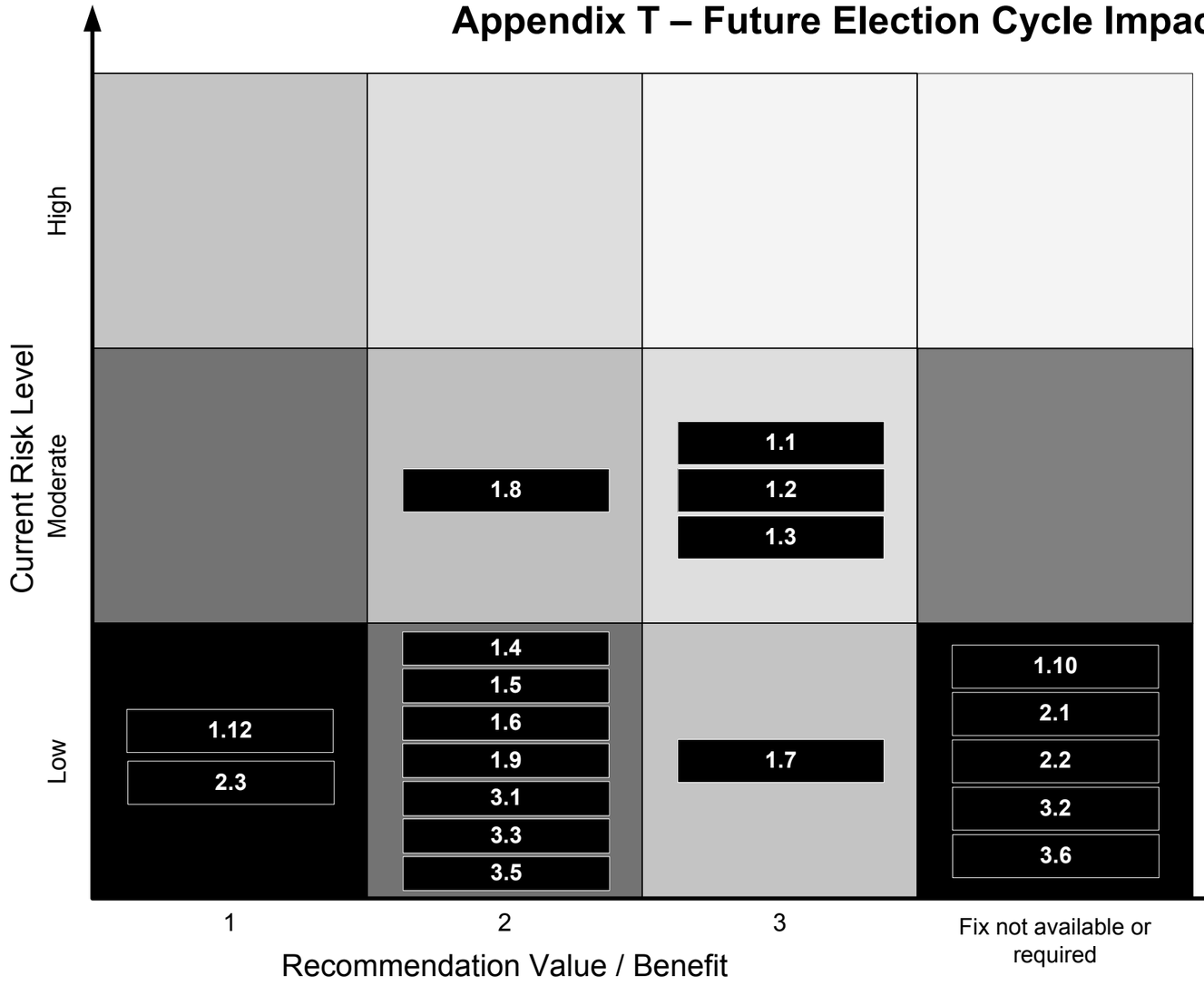


1.1 Assure 1.2 Upgrade Cost Analysis
1.2 Assure 1.2 Functionality Upgrade Analysis
1.3 Division of Elections Security Enhancements and Features Analysis
1.4 Implement procedures to minimize technology risks not addressed by existing or upgraded systems
1.5 Password Management
1.6 Chain of Custody
1.7 Best practices for equipment storage between elections
1.8 Trusted Personnel and single points of access
1.9 Redundancy
1.10 Paper Ballot tampering vulnerability
1.11 Master Vulnerabilty Matrix
1.12 Security Training
2.1 Communications Protocols, Integrity of hardware and software, perceived usability issues.
2.2 Preliminary Results Data Collection Assessment
2.3 Evaluate the reliability and accuracy of the optical scanning and touch screen systems in Alaska weather and transportation/handling conditions.
3.1 Procedures for functionaity, logic and accuracy testing for systems and memory cards.
3.2 Methods to improve voter confidence
3.3 Metrics and continuous improvement
3.4 Weekly email summary
3.5 Absentee and questioned ballot process
3.6 Random sampling methodologies

Residual Risk Level

Low | **Moderate** | **High**

Appendix T – Future Election Cycle Impact Matrix



1.1 Assure 1.2 Upgrade Cost Analysis
1.2 Assure 1.2 Functionality Upgrade Analysis
1.3 Division of Elections Security Enhancements and Features Analysis
1.4 Implement procedures to minimize technology risks not addressed by existing or upgraded systems
1.5 Password Management
1.6 Chain of Custody
1.7 Best practices for equipment storage between elections
1.8 Trusted Personnel and single points of access
1.9 Redundancy
1.10 Paper Ballot tampering vulnerability
1.11 Master Vulnerabilty Matrix
1.12 Security Training
2.1 Communications Protocols, Integrity of hardware and software, perceived usability issues.
2.2 Preliminary Results Data Collection Assessment
2.3 Evaluate the reliability and accuracy of the optical scanning and touch screen systems in Alaska weather and transportation/handling conditions.
3.1 Procedures for functionaity, logic and accuracy testing for systems and memory cards.
3.2 Methods to improve voter confidence
3.3 Metrics and continuous improvement
3.4 Weekly email summary
3.5 Absentee and questioned ballot process
3.6 Random sampling methodologies

Residual Risk Level

Low | **Moderate** | **High**

Appendix U: Photographs of System Components and Division of Elections Facilities

1.0 Alaska Division of Election Voting Equipment

AccuVote-OS (Optical Scan Terminal)

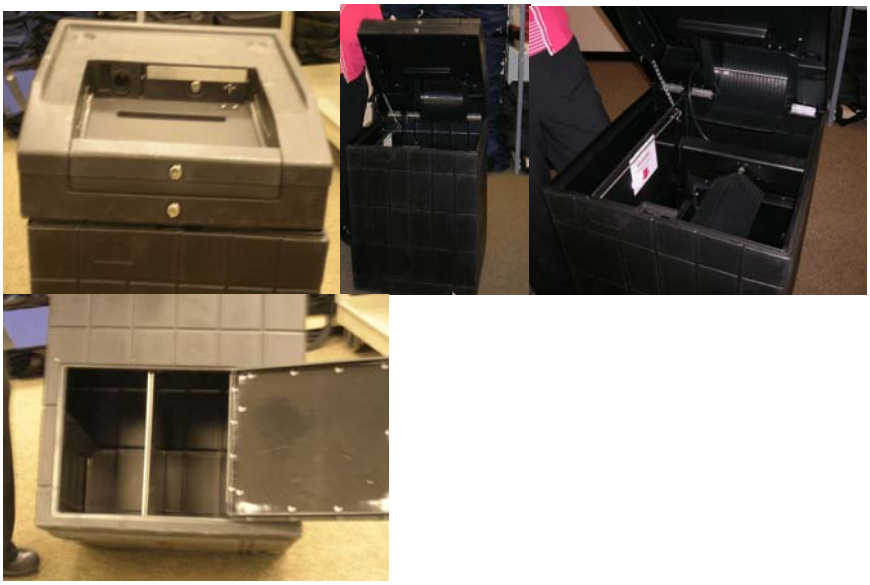
AccuVote-OS memory card port, memory card and panel to secure memory card in terminal.

Accuvote-OS Memory Card port secured with tamper evident, numbered tab. Tamper evident tab after removal.

AccuVote-OS Terminal vote recording tape chamber and tape. Tape is Secured beneath locked panel during election.

AccuVote-OS Terminal positioned over ballot container. Note lockable panel on ballot box is opened (lower left) . During election, locked front and rear panels of the ballot box coverthe secured memory card port and the rear of AccuVote OS unit (lower right).

Dual chamber, secure ballot container



Global Election Management System (GEMS) Server

GEMS Server (Fairbanks and Anchorage)

AccuVote-TXS (Touch Screen Voting Terminal)

AccuVote-TXS voting terminal, vote viewing panel and vote recording paper tape reel beneath lockable panel.

AccuVote-TXS voting terminal lockable memory card port and voter access card port.

2. Alaska Division of Elections Statewide, Regional and Borough Office's Equipment Storage

2.1 Juneau State-wide Office

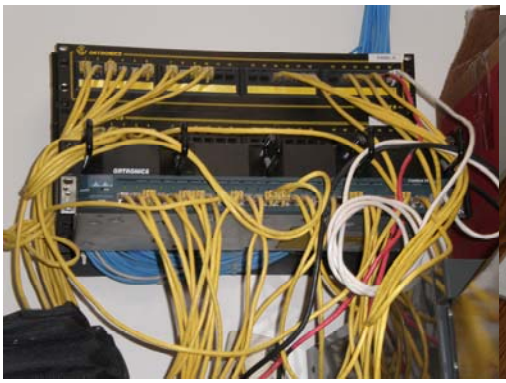
Election Programming Office keyed alarm panel and dead-bolt lock on door.

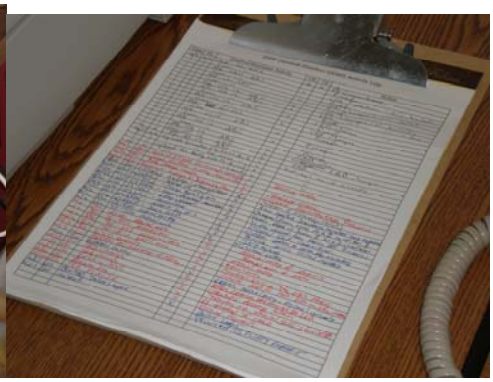
Election Programming Office Memory Card Storage Cabinet Memory Card Storage

Inside election programming office, GEMS Server and AV OS used for Memory Card programming prior to elections.

Inside AV-OS Unit: EPROM. Create barcode an place on underside of EPROM for security and inventory control

Switching Equipment in Election Programming Office and Equipment Action Log





Ballot Room

2.2 Region 1: Juneau

Alarm panel and memory card storage cabinet

GEMS Server

Walls and Ceiling

AV-OS Unit Storage

Inventory tags on shelves matched with individual AV-OS units.

AV-TSX Storage

2.3 Region 2: Anchorage

AccuVote-OS and AccuVote-TSX Storage areas.

AccuVote-TSX Voter Access Card programming units used at precincts. Numeric touch-pad alarm unit inside equipment storage room

2.4 Region 3: Fairbanks

(At the time of this photo the optical scanning equipment was on loan to the Fairbanks North Star Borough for their municipal election.)

2.5 Kenai Borough Office (Representative Hub)

Storage Vault

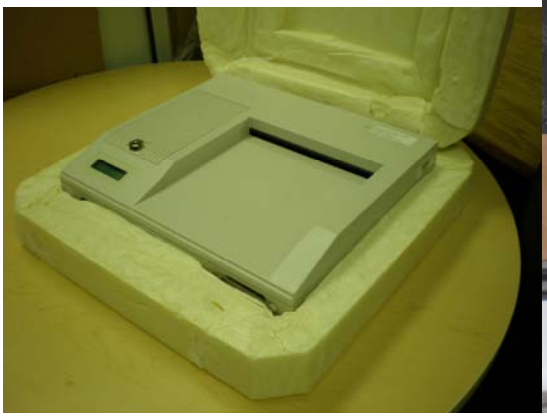
Equipment Storage inside Vault

Excess Election Material Storage

(Note: This material does not require secure storage (e.g. ballot boxes, tables, mailing envelopes, etc). No "secure" material is stored here (electronic equipment, ballots, etc.)

3.0 AV TSX and AV OS Shipping and Transportation

AV-OS foam padding and shipping boxes



AV-TSX Shipping Containers with locking capabilities

The AV-TSX shipping container plus the AV-TSX unit together weigh in excess of 50 pounds. The exterior latches on the AV-TSX shipping cases can be secured with serial-numbered tamper evident seals similar to the ones shown below.

AV-TSX Shipping Labels: US Mail Priority, Return Receipt