UAA

UNIVERSITY
of ALASKA
ANCHORAGE

State of Alaska Election Security Project Phase 1 Report

Final Revision with Integrated Executive Summary

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

December 21, 2007

This page left intentionally blank

Executive Summary
Alaska Election Security Report, Phase I

See the back page for a list of contributors

University of Alaska Anchorage

December 2007

Alaska voters depend on a chain of people and equipment to keep their votes secure—to count and report the votes accurately and protect the secrecy of individual ballots. How secure is Alaska's voting system? That's what Alaska's lieutenant governor and the Division of Elections asked the University of Alaska Anchorage to find out.

We're reporting here on the first phase of what will be a multi-phase study of Alaska's election security. The last phase will be completed before the 2008 presidential election.

What we found so far is in many ways re-assuring: Alaska's system has a number of features that address security. Paper ballots remain the official ballots, and they back up electronic counts. Vote counts are cross-checked in different locations. Alaska also has a centralized system for federal and state elections.

In this phase we also identified some areas where Alaska's system is potentially vulnerable. One important thing we did was review election-security studies done in California, Florida, and Connecticut, which use the same or similar election equipment as Alaska uses. Those studies identified a number of potential security issues with that equipment.

But studies that look only at voting equipment can't identify all the security issues Alaska might face—or how they might be mitigated by people and procedures. Also, Alaska's vast roadless areas and harsh winters create unique conditions—for instance, how might a touch-screen voting machine operate after sitting for hours on a remote runway at 30 degrees below zero?

We don't yet know enough to assess how real the threats are or to make specific recommendations. We've examined Alaska's election equipment and procedures and identified areas that need more evaluation.

Inside we summarize Phase I. But first we answer one of the questions voters often ask, since the vote-counting issues of the 2000 election—how are votes counted? Alaska has 439 polling places. In 149 of those, paper ballots are hand-counted. In the other 290, ballots are scanned and counted by machine. But the 149 precincts where ballots are hand-counted are small places—so only 6% of registered Alaska voters live where ballots are hand-counted .

Security Features of Alaska's Voting System

✓ *A single voting system, with standard procedures,* for federal and state elections throughout Alaska. This centralization is unique among the states and may offer fewer opportunities for tampering.

✓ *Identical hardware and software statewide.* Any flaws identified can if necessary be corrected throughout the system.

✓ *Paper ballots.* Almost all—99% of voters—still mark their choices on paper ballots. Even though votes are counted mostly by machine, the paper ballots provide a record in addition to electronic counts.

✓ *Bi-partisan committees* that oversee polling places and do hand-counts.

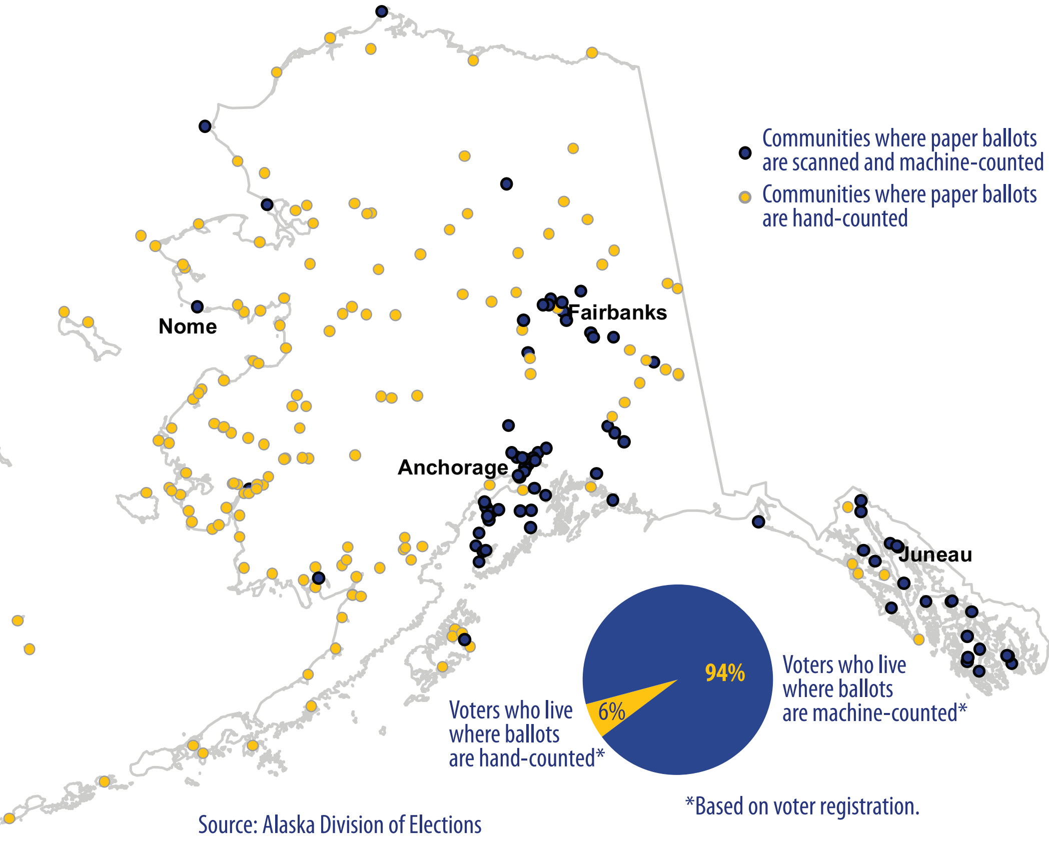
✓ *An open election process that by state law includes observers,* who are able to see both voting and counting procedures.

✓ *Verification of machine counts* with hand-counts of ballots from a random sample of precincts.

✓ *Physical separation of paper ballots and electronic tallies.* 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.

Source: Alaska Division of Elections

Map 1. How Do Alaska Voters Cast Their Ballots?



Nome
Fairbanks
Anchorage
Juneau
● Communities where paper ballots are scanned and machine-counted
● Communities where paper ballots are hand-counted
94%
6%
Voters who live where ballots are machine-counted*
Voters who live where ballots are hand-counted*

*Based on voter registration.

Source: Alaska Division of Elections

Background

Across the United States, Americans now typically use some type of electronic voting technology—for instance, optical scanners that scan paper ballots and count votes electronically, or touch-screen machines that don't involve paper ballots at all.

States have adopted that technology because it has a number of advantages over punch-ballots and other previous systems. Votes can be counted much faster, for one thing. Federal law also requires that every polling place in America have at least one machine for voters with disabilities that make it hard or impossible for them to mark paper ballots.

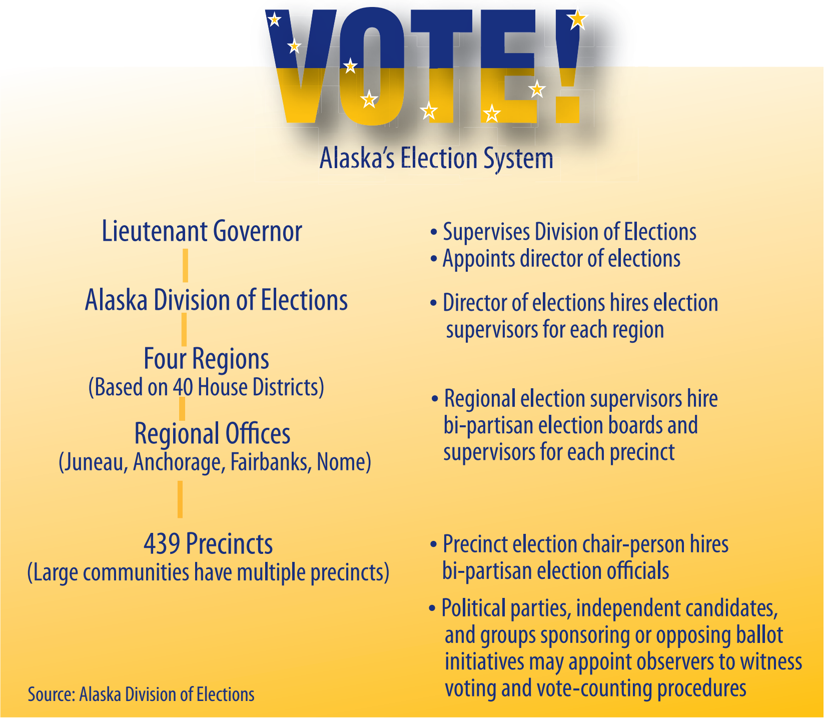
But a lot of Americans are worried that these electronic systems are vulnerable to attacks that could change the outcomes of elections. Many states have reviewed the security vulnerability of their systems. Recent studies in California and Florida found that the equipment and processes used in many states are vulnerable in various ways.

Alaska was among the first states to adopt electronic voting technologies, and today it uses the same or similar equipment as California and Florida and a number of other states. But there is good news in Alaska, which has already built a number of security features into its voting system. Those are summarized in the figure on the front page, and in important ways they contrast with situations in other states.

- Unlike in many other places, the overwhelming majority of Alaska voters—99%—still cast their votes on paper ballots, which serve as a back-up to electronic counts. By contrast, in California nearly 7 million voters rely on touch-screen devices alone.
- Alaska has a single voting system, with standard procedures, for federal and state elections throughout Alaska. That means the system is less complex, offers fewer opportunities for tampering, and any problems identified can be fixed statewide. By contrast, in California, counties can determine their own election procedures.
- A state review board verifies machine-counts with hand-counts from a random sample of precincts. If the results vary by more than 1%, votes from all precincts in the district will be hand-counted. But in most other states, cities and counties manage elections at all levels and only report results to a statewide office.

Still, despite these security features, the lieutenant governor and the Division of Elections are aware of the studies showing vulnerabilities in other states. The division has internally identified some potential risks in the Alaska system and taken steps to deal with them. But the lieutenant governor and the division want Alaska's elections to be as secure as possible—so they asked for this study, to help them identify and correct any security concerns in Alaska's election technology or processes.

Many of the existing election-security studies look only at the vulnerability of electronic systems—and it is electronic technology that gets most of the attention in national debates about election security. But in this study, we are looking at the entire election system—not only the technology but the election policies and procedures. All parts of the system are inter-related, all parts are critical to the election process—and the system can be vulnerable at any point.



VOTE!

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

In this first phase of the project, we did several tasks:

- Examined Alaska's voting system, including equipment and procedures.
- Did detailed reviews of election-security studies for California and Florida and interviewed researchers who conducted those studies.
- Identified areas of Alaska's system that need more evaluation.

Below we start by describing Alaska's system: the election framework, the technology used, and the voting system during elections.

Alaska's Election Framework

The figure at the top of the page shows the framework of Alaska's system. The lieutenant governor heads the election system, supervising the state Division of Elections and appointing the director of elections.

The Division of Elections manages Alaska's state and federal elections on a statewide basis, which is unusual among the states. As we pointed out earlier, in most places cities and counties manage federal, state, and local elections and simply report their election results to a statewide office. (In Alaska, cities and boroughs manage only local government elections.)

Alaska's Division of Elections has four regions, with offices in Juneau, Anchorage, Fairbanks, and Nome. Those regions are based on the boundaries of the 40 state house districts. The regulations, procedures, training, and technology are all the same throughout the state.

The statewide director of elections hires election supervisors for each region, and those regional supervisors in turn hire bipartisan election boards and supervisors for each of the 439 precincts where Alaskans go to cast their ballots.

At the precinct level, the precinct election chair-person hires bipartisan election officials. A wide range of groups—including independent candidates and supporters and opponents of ballot initiatives—can appoint observers to watch the voting and vote-counting procedures.

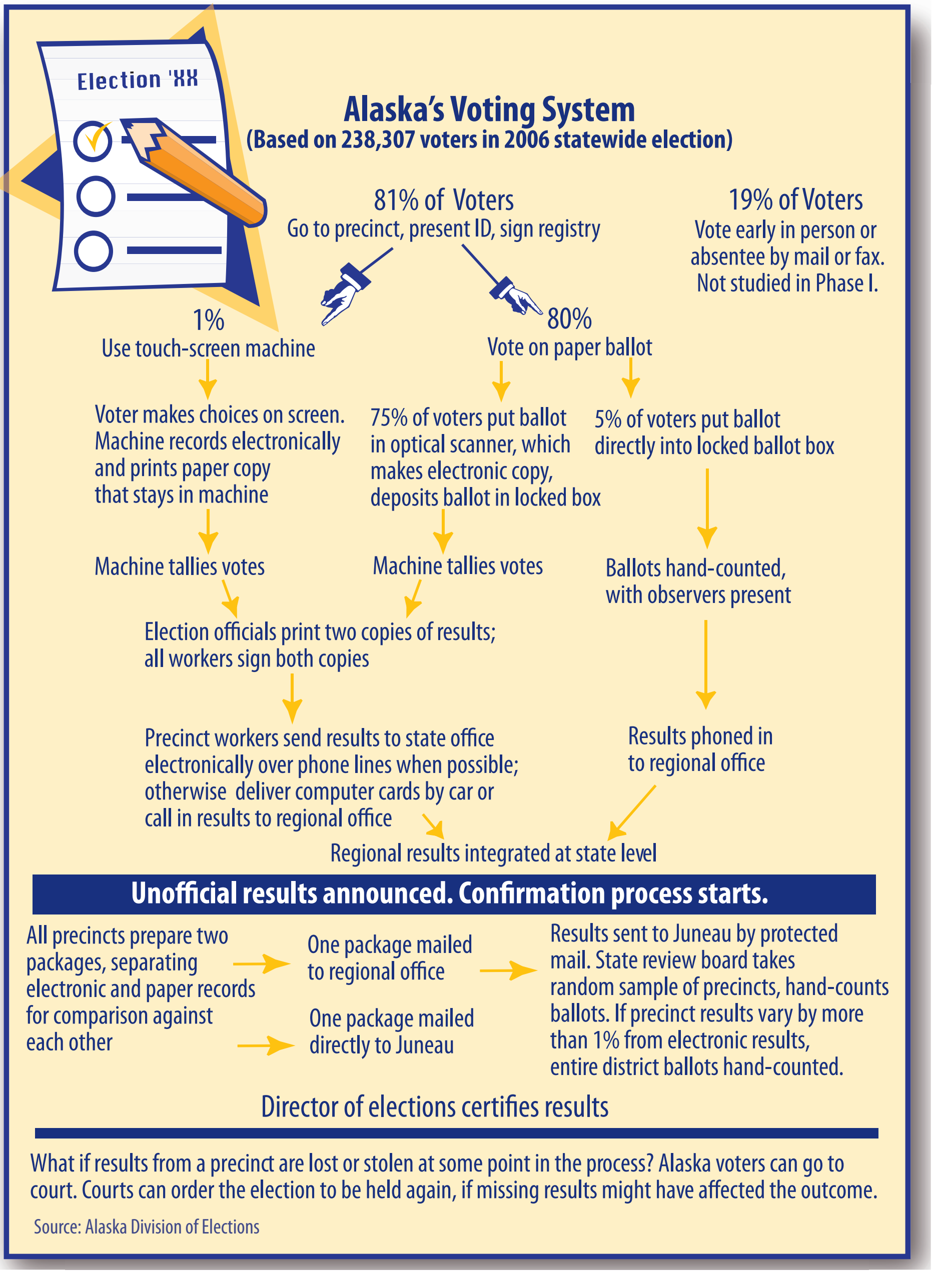
What Technology Does Alaska Use?

- **Optical scanners** scan paper ballots and count the votes. Voters mark their choices on paper ballots and slide them into the optical scanner. After the ballots are scanned, they drop into a locked box below the scanner. Scanners are used in 290 of Alaska's 439 precincts. Votes are hand-counted in the remaining 149 precincts.
- **Touch-screen machines** are equipped with printers but don't involve paper ballots. Voters touch a screen to make choices. The machine then prints and displays a paper copy, for the voter to verify, but the paper scroll stays in the machines. All 439 Alaska precincts have these devices, as required by federal law, but only about 1% of Alaska voters use them.
- **Computer servers** that run election system software, integrate election results at the regional and state levels, and execute other election-related tasks. These are at the statewide office and the four regional offices. They are not connected to the public Internet.

The Voting System

The adjacent figure summarizes the multiple steps in the voting system, from the time Alaskans go to the polls until the statewide director of elections certifies the results.

The vote percentages shown in the figure are based on the roughly 238,000 Alaskans who voted in the 2006 election. (This is different from the approximately 465,00 Alaskans who were registered to vote in 2006.) About 19% of Alaskans voted early or absentee, and 81% went to the polls on election day.



Alaska's Voting System

(Based on 238,307 voters in 2006 statewide election)

81% of Voters
Go to precinct, present ID, sign registry

19% of Voters
Vote early in person or absentee by mail or fax. Not studied in Phase I.

1%
Use touch-screen machine

Voter makes choices on screen. Machine records electronically and prints paper copy that stays in machine

Machine tallies votes

80%
Vote on paper ballot

75% of voters put ballot in optical scanner, which makes electronic copy, deposits ballot in locked box

Machine tallies votes

5% of voters put ballot directly into locked ballot box

Ballots hand-counted, with observers present

Results phoned in to regional office

Election officials print two copies of results; all workers sign both copies

Precinct workers send results to state office electronically over phone lines when possible; otherwise deliver computer cards by car or call in results to regional office

Regional results integrated at state level

Unofficial results announced. Confirmation process starts.

All precincts prepare two packages, separating electronic and paper records for comparison against each other

One package mailed to regional office

One package mailed directly to Juneau

Results sent to Juneau by protected mail. State review board takes random sample of precincts, hand-counts ballots. If precinct results vary by more than 1% from electronic results, entire district ballots hand-counted.

Director of elections certifies results

What if results from a precinct are lost or stolen at some point in the process? Alaska voters can go to court. Courts can order the election to be held again, if missing results might have affected the outcome.

Source: Alaska Division of Elections

About 75% of those who voted did so in precincts where votes are machine-counted and 5% in precincts where votes are hand-counted. The other 1% used touch-screen devices, which are in all polling places.

Notice that at all steps of the process there are procedures intended to help protect the integrity of votes. Those include:

- Paper ballot back-ups or paper records for all votes.
- Bipartisan committees that oversee polling places and conduct hand-counts.
- Observers who can see both the voting and the vote-counting procedures.
- Verification of machine-counts with hand-counts of ballots from a random sample of precincts.
- Physical separation of paper ballots and electronic tallies, for independent cross-checking at the state level.

What Does Security Mean?

Even though Alaska's election system may have security advantages over those in some other places, there are points in all systems where security can fail. And while potential problems with electronic voting systems get most of the attention, systems using paper ballots can also pose risks.

Security failures can be related to computer hardware or software, to procedures, or to transport, storage, and use of voting equipment. For instance, hackers could change software to alter individual votes or vote counts. Ballots could be lost in the mail. Equipment stored in unsecured locations could be tampered with or stolen.

Also keep in mind that "security" is not the same in all places at all times—it has to be evaluated in context.

- What are the capabilities and motives of potential attackers?
- What's the environment where the system will be used?
- What's the level of trust in the components of the system and the people who administer them?
- What are the types and values of the assets to be protected?

And finally, while we generally think of "security" as the capacity of the system to accurately record and report the intent of the voters, there's another critical element to security. The public needs to have confidence in the system. Even if the system works at an acceptable level, the people who administer it have to be able to demonstrate to the public how and why specific election results were produced.

What Did the California and Florida Studies Find?

As part of Phase I, we reviewed a number of election-security studies done in other states. But our reviews of the California and Florida studies were the most detailed—and those states use the same or similar electronic equipment as Alaska. Generally speaking, the studies identified a number of worrisome vulnerabilities, including:

- Vulnerability to the installation of malicious software that could allow incorrect recording or miscounts of votes.
- Susceptibility to computer viruses that could spread from voting machine to voting machine and to election management systems.
- Insufficient control of access to and management of machines, potentially making them accessible to unauthorized people.

The manufacturer of the equipment—Premier Election Solutions—made improvements in its software and machines, based on these studies. Follow-up studies by Florida investigators found that newer versions of Premier software and hardware corrected some but not all the flaws identified.

What About Alaska?

We've noted that Alaska's election procedures afford the state a degree of consistency—and those procedures could help mitigate the potential vulnerabilities in electronic voting equipment. Nevertheless, the equipment is a critical part of the election system. Phase II of the Alaska Election Security Report will examine the system's technical components in the context of Alaska's entire election system.

Proposed Phase II Approach

For the second phase of this project, we propose further research in a number of areas that represent a variety of potential risks to the election system—and to the public trust in that system. We can think of a secure system as having three inter-related parts, and we'll group our proposed research into those three categories.

Defense in Depth. By that we mean a secure system should have multiple layers of protection—so if one layer fails, others will still be standing. To improve defense in depth, we propose to:

- Inventory the software on all voting machines and verify that all are running the same version, and evaluate the cost and process to upgrade existing systems if newer versions are available and certified before the 2008 election cycle.
- Document and map where election equipment is stored from one election to the next, looking at how the equipment is stored, when it is loaned to municipalities, and where it is repaired. Document security practices in regional offices and hub communities. Determine best practices for storage, and whether they would be feasible in all Alaska communities.
- Document and map the chain-of-custody for voting equipment from one election cycle to the next. Determine when machines are out of that custody, including transportation to and storage at election workers' houses, and assess risks of tampering, damage, or loss.
- Evaluate whether voting procedures are correctly implemented in polling places and identify ways polling places could reduce security risks.
- Assess security training by the state and Premier Election Solutions.
- Identify trusted personnel in the election system and their points of access to equipment. Identify any points where only one person has access.
- Identify areas of risk in Alaska's absentee and questioned ballot system.
- Assess vulnerability of paper ballots to tampering, and contrast with risks in electronic system.
- Determine points in the election system where there should be more redundancy in personnel or procedures.

Fortification of Systems. Here we mean making electronic systems as secure as possible and using the latest certified updates, which may correct vulnerabilities found in earlier systems.

- Assess the communication protocols used in the electronic voting system, the integrity and reliability of hardware and software, and the perceived and real usability features.
- Evaluate changes and potential enhancements in election systems that other states have made and help determine their costs and benefits.
- Analyze technical processes in place, including configuration options; review technical documentation; and investigate how conditions unique to Alaska affect the security of the technical processes.

Confidence in Outcomes. This means having systems and results that can be verified and shown to be reliable—and therefore maintaining the public's trust and increasing the confidence of election officials. Given the widespread distrust of electronic voting systems, this is critical.

- Review public comments on Phase I and incorporate them as appropriate into Phase II research. Identify methods to increase voter confidence.
- Identify alternate methods for selecting random samples and hand-counting ballots, to determine if they would be more effective than current methods.
- Audit system security, before and after elections. Evaluate processes for testing functionality, logic, and accuracy.
- Do a weekly review of e-mails from the public on security issues and summarize and publish general responses to them. We will not be able to respond to individual e-mails.

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

Introduction

Most states that use electronic voting technologies have reviewed the security vulnerabilities of their elections processes and equipment in response to increased concerns from the public. Studies in California, Florida, Connecticut, Maryland, Ohio and others have reported worrisome vulnerability levels in equipment used in many other states.

Alaska was one of the first states to adopt electronic voting technologies, almost ten years ago. Lieutenant Governor Sean Parnell and the Division of Elections are strongly committed to election security and voter confidence in the state. In support of this commitment, they have commissioned the University of Alaska Anchorage to evaluate Alaska’s current election systems and processes to identify security issues that could jeopardize election results. The purpose of this evaluation is to understand relevant issues which require action to ensure the integrity of the results and maintain the public trust.

A team of experts from the University of Alaska and industry, representing critical knowledge areas, produced this report. Experts from University of California, Florida State University, California Institute of Technology and the University of Connecticut provided an independent review of the document.

The report is an overview-level evaluation of recent studies and a determination of their relevance to Alaska’s systems, technologies, and procedures. It is the first part of a multi-phase project to evaluate the security of Alaska's election system[1]. The research includes a detailed study of the evaluation reports from California, Florida, Maryland, Ohio and Connecticut, a review of the response to the California study by equipment provider Premier Election Solutions(formerly Diebold) , and an overview of Alaska's election laws and procedures. The team conducted interviews with members of the University of California and Florida State University evaluation teams, with officials from the State of Alaska Division of Elections, and with election officials from California, Florida and Connecticut. As a result of this Phase 1 work, the research team identified areas within the election system and equipment used that warrant further analysis necessary to develop more definitive conclusions.

California, Florida, Connecticut, Maryland and Ohio conducted their studies using equipment that is also used in Alaska. These evaluations found serious technical vulnerabilities in the systems studied. Most reports also point out that procedures have the potential to either mitigate or exacerbate vulnerabilities reported at the equipment level. Many of these items have been proactively flagged by the officials in the Division of Elections. As appropriate, they have implemented measures and identified possible approaches to address some of these vulnerabilities.

Each state in the US can adopt processes and procedures to meet their unique requirements. They can also select from a range of vendors and equipment provided federal certification standards have been met. Given the wide range of implementations, it is critically important that all system and procedural issues be investigated carefully in the context of policies and procedures in place in the state in which they are evaluated. In Alaska, this approach is essential to determine what, if any, impacts these issues have on the security of elections in Alaska. The use of paper ballots as the primary record of votes, the procedures for hand recounts and the uniform practices across the state may reduce vulnerabilities in Alaska elections.

[1] For the purpose of this report, security is defined as the ability of the election system to accurately reflect the intent of the authorized voters while preserving the secrecy of any individual’s vote.

The Phase 2 evaluation will build on the foundation of knowledge developed in Phase 1. This Phase 1 knowledge includes an understanding of the technical limitations and vulnerabilities of the equipment and an understanding of the processes and procedures currently in place. The additional knowledge and proposals developed in Phase 2 will seek to build additional confidence in the integrity of the overall election process.

The research team recommends the following areas for in-depth analysis in Phase 2:

1. "Defense in Depth": The concept of Defense in Depth was developed by the National Security Agency. It is an approach that requires an attacker to break through multiple layers to breach the security of a system. A layered approach, including well-placed policies, procedures and security mechanisms, can increase the dependability of the system and assist with early detection and prevention of attacks. This approach has been used very effectively in the Information Technology arena. Its application to election security seems appropriate.

    - The election system may have points of vulnerability that can be exploited. These include chain of custody, access, transportation & storage, training, trusted personnel, lack of redundancy and review, etc.

        - Study processes, procedures and personnel policies to expose vulnerabilities. Assess the degree of probability and impact on the overall election system. Propose approaches (including evaluation of suggestions made by Division of Elections) to appropriately mitigate prioritized risks.

        - Establish a set of election security metrics that can be used to assess and be the foundation for continuous improvement efforts.

2. System Fortification:

    - Systems should incorporate best-available, certified functionality and capabilities.

        - Evaluate changes to equipment made in response to California and Florida studies. Conduct cost/benefit analysis. As appropriate, develop approach to efficiently upgrade existing equipment. Identify technology and equipment reliability risks unique to Alaska. Propose approaches to address these issues.

3. Confidence in Outcomes

    - The Election System (processes, personnel and equipment) should work in concert to deliver predictable, credible and repeatable results leading to increased levels of confidence by the public and election officials

        - Identify sources of low-confidence (real and perceived). Develop procedures and communication mechanisms to assess and increase confidence. Implement methodologies that can demonstrate repeatable, credible and verifiable results.

The election equipment evaluated in the California and Florida studies and also used in Alaska is provided by Premier Election Solutions (formally Diebold):

Global Election Management Systems (GEMS®,: a server that runs election systems software and executes various election related tasks in combination with the AccuVote®-TSX and the AccuVote®-OS systems. The firmware version for GEMS® is 1.18.24.0. Five of these systems are used in Alaska at regional and state-wide level.
AccuVote®-TSX , a touch-screen direct recording electronic (DRE) voting terminal, comprised of Ballot Station Version 4.6.4, Bootloader Version BLR 7-1.2.1, and Vote Card Encoder 1.3.2. There are 439 of these systems used in Alaska, one at each voting precinct.
AccuVote®-OS, a precinct and central accumulation optical scan voting system, version 1.96.6, and AccuFeed Device (paper ballot feeder). These systems are used in 290 precincts across Alaska. The remaining precincts conduct a hand count of their paper ballots.

Disclaimer

This work represented in this report was based on current, publicly available reports as well as interviews with key election personnel, documentation reviews, and demonstrations of election systems. Neither an in-depth, hands-on analysis of the equipment nor a direct observation of Alaska's election processes and procedures was conducted. Therefore, until a more detailed Phase 2 analysis is conducted, the team cannot draw specific conclusions or make definitive recommendations for Alaska's specific environment.

Table of Contents

This page left intentionally blank

1 Project Overview

Alaska’s lieutenant governor, Sean Parnell, and the personnel of 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. This report presents the findings of Phase 1 of the Election Security Project. Below we first briefly describe the background of the project and then describe the approach we used in Phase 1.

Across the United States, Americans now typically use some type of electronic voting technology—for instance, optical scanners that scan paper ballots and count votes and touch-screen machines that don’t involve paper ballots at all. States have adopted that technology because it has a number of advantages—votes can be counted much faster, for one thing—and because federal law requires that all polling places have at least one machine for voters with disabilities.

But many Americans are worried that these electronic systems aren’t secure—that they’re vulnerable to attacks that could change the outcome of elections. A number of states have reviewed the security vulnerability of their systems. Recent studies in California and Florida reported that equipment and processes in common use throughout the country are vulnerable in various ways.

Alaska was among the first states to adopt electronic voting technologies, and today it uses the same or similar technology as California and Florida. But there is good news in Alaska, which has already built a number of security features into its voting system.

- Unlike voters in many other places, the overwhelming majority of Alaska voters—99%—still cast their votes on paper ballots, which remain the official ballots and serve as a back-up to electronic counts. By contrast, in California nearly 7 million voters rely on touch-screen devices alone.
- Alaska has a single voting system, with standard procedures, throughout the state. That means the system is less complex and offers fewer opportunities for tampering. In California, counties can determine their own election procedures.
- A state review board verifies machine counts with hand-counts from a statistical sample of precincts. If the results vary by more than 1%, votes from all precincts in the district will be hand-counted.
- Bi-partisan committees oversee polling places, and political parties, independent candidates, and supporters or opponents of ballot initiatives can appoint observers who can witness both voting and counting procedures.

Alaska’s lieutenant governor—who oversees election process—and the Division of Elections are aware of existing research showing vulnerabilities in election systems. The division has internally identified some potential vulnerabilities, and taken steps to deal with them. But both the lieutenant governor and the division are committed to making Alaska’s voting system as secure as possible. That’s why they asked for this study: to help them identify and correct any security vulnerabilities in the technology or the processes used in Alaska’s election system.

1.1 Project Objectives

This project, the 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.

The multi-phase project will identify whether technology, system, or procedural vulnerabilities exist and recommend solutions. It’s important to emphasize here how our study differs from most previous evaluations of election security: we are looking not only at electronic systems but at the entire system—the policies and procedures the state has in place. And while it is the electronic technology that has received the most attention in national debates about election security, the policies and procedures—and the people responsible for carrying them out—are critical parts of any security system.

To help us think about what constitutes a secure system, we can divide it into three inter-related parts:

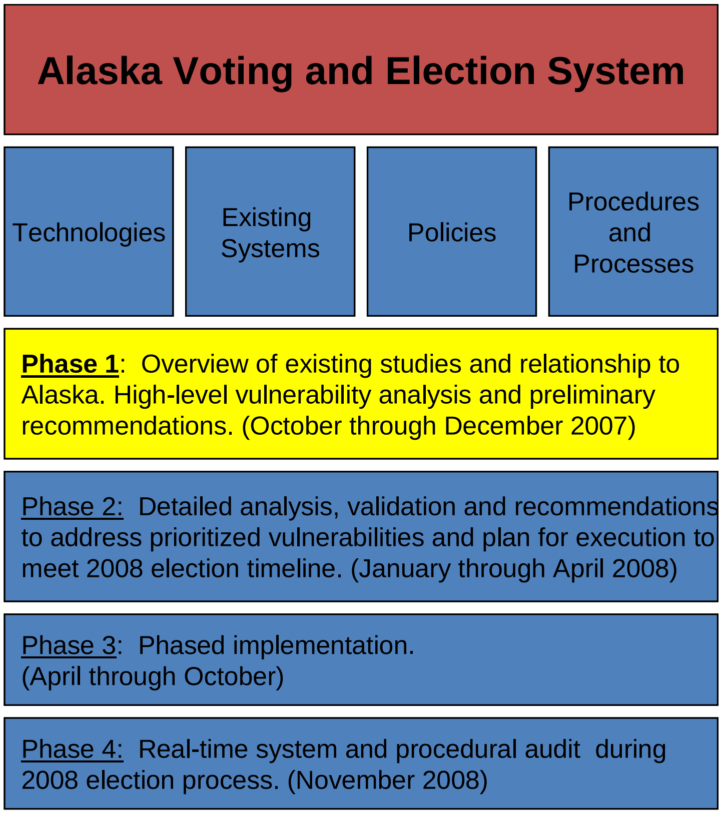
- Defense in depth. By that we mean a secure system should have multiple layers of protection—so that if one layer fails, others will still be standing. So for one simple example, in Alaska electronic tallies of votes are backed up by paper ballots, measures are taken to keep the voting machines secure, and electronic counts are verified through hand-counting a random sample of ballots.

- Fortification of systems. Here we mean making electronic systems as secure as possible and using the latest updates, which often correct some vulnerabilities found in earlier systems. Also, we need to understand the implications of Alaska’s unique conditions—for instance, voting machines may have to sit for hours on remote runways at 40 degrees below zero—that may require special considerations.

- Confidence in outcomes. This means having systems and results that can be verified and shown to be reliable—and therefore earning 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 observe how it works and informing them about problems identified and solutions.

1.2 Multi-Phase Project

This project will have several phases, timed to coordinate with the 2008 election process. We decided to carry out the Alaska study in phases, after consulting with teams from the University of California and Florida State University who evaluated election security in those states. This approach provides an opportunity to leverage existing work and identify areas for further evaluation. We’ll do progressively more detailed analysis of those areas, putting priority on those that seem most vulnerable. Figure 1 shows the tasks in each phase and the projected timing.



Alaska Voting and Election System

Technologies

Existing Systems

Policies

Procedures and Processes

Phase 1: Overview of existing studies and relationship to Alaska. High-level vulnerability analysis and preliminary recommendations. (October through December 2007)

Phase 2: Detailed analysis, validation and recommendations to address prioritized vulnerabilities and plan for execution to meet 2008 election timeline. (January through April 2008)

Phase 3: Phased implementation.
(April through October)

Phase 4: Real-time system and procedural audit during 2008 election process. (November 2008)

Figure 1 – Multiphase approach to Alaska Election Security Project

1.3 Phase 1 Scope of Work

Phase 1 of this study includes the following major tasks:

- Briefly review previous studies and tests that might be relevant to Alaska's situation.
- Summarize the tests and conclusions of the University of California and Florida State University studies, and analyze the recommendations they made that are applicable to Alaska's optical scanning and touch screen voting and tabulation systems.
- Assess improvements made by Premier Election Solutions (formerly Diebold) based on the California and Florida studies and their applicability to our systems.
- Assess existing Alaska systems and equipment and the ability to upgrade their security functionality
- Look at other states conducting similar research, to determine potential points of collaboration, partnership and leverage
- Do a general evaluation of Alaska's election policies, processes, and procedures
- Provide a repository for public input via the Division of Elections Web site, and use this input to guide the suggested approach for interactive public input/response in Phase 2. Ensure that both UAA and Division of Elections have a record of public input.

1.4 Phase 1 Approach

Our approach to this first phase of work included research by an expert team from across organizations; interviews with key researchers, personnel of the Alaska Division of Elections, and others; and review and evaluation of a variety of documents related to election security.

Cross-Organizational Expert Team

We assembled a team of experts from the University of Alaska and industry with knowledge in areas critical to this study.

Principal Investigator

LuAnn Piccard, PMP, Instructor and Program Development Director, Engineering, Science and Project Management Department, School of Engineering, University of Alaska Anchorage

Technical Team

Mark Ayers, P.E. (Technical Team Investigator), Systems Engineer and Adjunct Faculty Member, University of Alaska Anchorage

Kerry Digou (Technical Team Investigator), Chief Security Officer, University of Alaska-Statewide

Dr. Bogdan Hoanca (Technical Team Investigator), Associate Professor of Management Information Systems, College of Business and Public Policy, University of Alaska Anchorage

Dr. Kenrick Mock (Technical Team Investigator), Associate Professor of Computer Science, College of Arts and Sciences, University of Alaska Anchorage

Process, Procedures, and People Team

Dr. David B. Hoffman, (Process Team Senior Investigator), Adjunct Faculty and Consultant, University of Alaska Anchorage; retired Professor of Business Administration, University of Alaska Fairbanks. Dr. Hoffman was the development director for the Arctic Region Supercomputing Center during his tenure at the University of Alaska Fairbanks.

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

External Document Review Team

Dr. Michael Alvarez, Professor, Division of Humanities and Social Sciences, California Institute of Technology; Caltech/MIT Voting Technology Project Co-Director

Dr. Matthew Bishop, Professor, Computer Science Department and Co-Director, Computer Security Laboratory, University of California Davis; California Top to Bottom Review (TTBR) “Red-Team” evaluation leader

Dr. Alexander Shvartsman, Professor, Computer Science and Engineering, UConn Voting Technology Research Center (VoTeR Center), University of Connecticut

Dr. David Wagner, Associate Professor, Computer Science Division, University of California Berkeley; Principal Investigator for Source Code Review of the Diebold Voting System for the California Top-to-Bottom Review.

Dr. Rich Whitney, Chief Information Officer and Vice Provost for Information Technology, University of Alaska Anchorage

Dr. Alec Yasinsac, Associate Professor, Computer Science Department and co-founder and co-director of the Security and Assurance in Information Security (SAIT) Laboratory, Florida State University; Principal Investigator for the Software Review and Security Analysis of the Diebold Voting Machine Software Report and Supplemental Report produced for the Florida Department of State, Division of Elections

Interviews with Key Researchers from California, Florida and University of Alaska Fairbanks

The team conducted several in-depth interviews with members of the evaluation teams from the University of California and Florida State University. Insights from these discussions helped the Alaska team understand the California and Florida research and its applicability to Alaska. We especially thank several of those researchers for their generous contribution to our study—Dr. Matt Bishop from University of California Davis, Dr. David Wagner from the University of California Berkeley, Dr. Alec Yasinsac from Florida State University, and Dr. Michael Alvarez from the California Institute of Technology. Additionally, we also thank Dr. Brian Hay, Dr. Orion Lawlor, and Dr. Kara Nance from the University of Alaska Fairbanks, Computer Science Department and Advanced System Security Education, Research and Training Center (ASSERT), which is a NSA/DHS designated Center of Academic Excellence in Information Assurance Education.

Interviews with Members of the Alaska Division of Elections

We also conducted detailed interviews with members of the Alaska Division of Elections team. We thank several people for their openness and sharing of information on Alaska election policies, processes, and procedures: Whitney Brewster, director, Division of Elections; Shelly Growden, manager, HAVA Election Systems; Carol Thompson, manager, Absentee and Petition Manager; Denali Elmore, Election Supervisor Region 2 (Anchorage and Mat-Su); and Becka Baker, Election Supervisor Region 4 (Nome Region). In addition, special thanks are in order for staff members who conducted several hands-on equipment demonstrations for us during three team visits to Division of Elections offices in Fairbanks and Anchorage.

Other Interviews and Document Reviews

- Interviews with Leslie Mara, Connecticut Deputy Secretary of State; Steven Weir, president, California Association of Clerks and Election Officials; and Sarah Jane Bradshaw, Acting Director, Florida Division of Elections
- Evaluation of Alaska systems configurations and revision levels, compared with systems studied in California and Florida reports
- Detailed study of University of California and Florida State University election-security reports
- Review of Maryland, University of Connecticut and Ohio reports
- Review of the Federal Elections Commission Voting Systems Performance and Test Standards
- Review of follow-up response from Premier Election Solutions (formally Diebold) resulting from the California study
- Interviews and discussions with Premier Election Solutions staff and development team.
- Review of Alaska Election Laws and Regulations (2006-2007 Edition)
- Interviews with SysTest, a federally approved Independent Test Authority (ITA) which conducts independent election equipment certification and conformance test evaluations.
- Integration of data, information, reports, and other materials

Phase 1 Exclusions

Due to limited time and staff resources, we were only able to assess some aspects of Alaska's voting system in Phase 1. Specifically, we ***did not***:

- Do a detailed analysis, hands-on operational and technical evaluation of systems
- Conduct a detailed study of Alaska's election policies, processes and procedures
- Directly respond to public input
- Evaluate usability issues related to using touch-screen systems, including ease of use, training, set-up, removal, quality, and transportation
- Conduct a detailed study of process for absentee and questioned ballots
- Study the voter registration process

2 Alaska’s Historical Perspective

2.1 How Did We Get Here?

Understanding how Alaska’s current electronic voting system evolved is important. It places that system in a broader context, helps us understand the threats to our system compared with threats other states face, and explains why some parts of the system can’t be changed.

The Florida recounts following the presidential election in 2000 triggered a large-scale implementation of electronic voting across the United States. Most voting districts around the country used punch card ballots during that election, and Florida was no exception. After the votes were counted in Florida, George Bush led Al Gore by only 1,784 votes—and as it turned out, the presidential election hinged on the Florida results. Because those results were so critical, and the difference in votes for the two candidates was so small, the Florida State Supreme Court ordered a recount in several counties. The problems with punch card ballots became evident during that recount. Counting machines used in some places did not count partial perforations (the infamous hanging chads) that hand counts in other places were able to identify. The U.S. Supreme Court halted the recount, noting that different recounting methods in different places violated the principle of one person, one vote.

In 2002, President Bush signed the Help America Vote Act (HAVA) into law. The HAVA legislation sought to improve the administration of elections through three primary means: creation of the Election Assistance Commission (EAC) to act as a clearing house for election administration information; provide funds to improve election administration and replace outdated voting systems; and create minimum standards for states to follow in several key areas of election administrations. (Source: US Department of Justice Voting Section Home Page). In addition, the HAVA standards mandated that each polling place have at least one machine accessible for people with disabilities and provided funding for such machines. After the law was passed, the Congressional Research Service determined that touch-screen machines were the only machines available that fulfilled the accessibility requirements of HAVA.

2.2 Alaska's Move to Electronic Voting

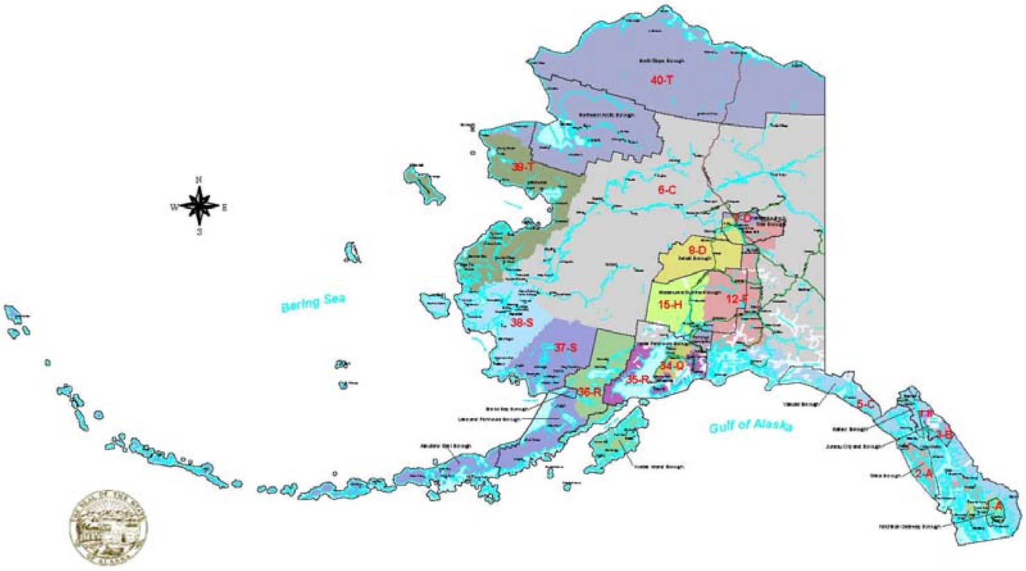
Alaska was one of the first states to move away from punch cards and adopt electronic voting technologies, a decade ago. After determining that Alaska’s outdated punch-card ballot system was vulnerable to failure, the lieutenant governor and Division of Elections undertook an evaluation of alternative voting systems. They chose optical scanning of paper ballots and implemented that system in time for the 1998 election. The system has remained in place and has functioned reliably ever since.

Initiated in 2003 and completed in 2005, the state purchased one touch-screen device for each of Alaska’s 439 polling places, in accordance with HAVA requirements. Those touch-screen devices are primarily intended for voters with disabilities (although other voters may use them as well). Less than 1% of Alaska votes are cast using touch screen devices, making Alaska’s reliance on electronic devices among the lowest in the country. Much of the public concern about vulnerabilities in elections systems centers on touch-screen devices, which are not backed up by paper ballots.

2.3 Election Districts, Regions, and Precincts

Alaska's state and federal elections are managed on a statewide basis by the Division of Elections, which is unusual among the states. In most places, cities and counties manage elections and only report their results to a statewide office, usually the Secretary of State. Alaska's Division of Elections has four regions with offices in Juneau, Anchorage, Fairbanks and Nome. The regulations, procedures, training and technology are all the same throughout the state.

As indicated in the following map, there are 40 house districts composed of 439 precincts. All 439 precincts have touch screen devices, and 290 also use optical scanning machines to count ballots. The remaining 149 precincts hand count their ballots.[2] Precincts with large populations use optical scanners to count votes more rapidly. In 2007, about 94% of registered voters (approximately 448,000 of 477,000 total registered voters) live in precincts where votes are counted by optical scanning machines. The remaining voters (approximately 29,000) live in precincts where votes are counted by hand. Touch screen devices are intended primarily for voters with disabilities but because at least five votes are desired for voter confidentiality, other voters are given the option of using them as well.



Amendments adopted by Alaska Redistricting Board
April 13 as modified on April 18, 2002

Prepared by Alaska Redistricting Board
April 25, 2002

Source: Alaska Redistricting Board. *http://www.elections.state.ak.us/maps.php*.

Figure 2. Alaska State House Districts

[2] http://ltgov.state.ak.us/elections/

3 Election Security

3.1 Definition of Security

Security should never be considered an absolute, but rather must be considered in the context of its environment. No statement about the security of a system should be taken seriously unless it includes some information about:

- The capabilities and motivations of the potential attackers
- The environment in which the system will be deployed
- The degree to which the participants and components of the system are trusted
- The type and value of the assets being protected

Elections should reflect the intent of the voters while preserving the secrecy of any individual's vote. But there are points in all election systems where things can go wrong. That includes both paper-based and electronic voting systems, and systems that have been in use for years.

- A voter accidentally casts a ballot incorrectly (e.g., a voter intended to vote for Alice, but checked the box for Bob).
- A ballot is modified after it has been cast (e.g., a ballot which contains a vote for Alice is modified so that it contains a vote for Bob).
- A vote is attributed incorrectly (e.g., a vote for Alice is incorrectly counted as a vote for Bob).
- The results of the election are modified or reported incorrectly (e.g., more voters cast votes for Alice than for Bob, but Bob is incorrectly declared to be the winner when the final totals are attributed to the wrong candidates).
- The vote cast by a specific voter can be determined (e.g., papers ballots are stored in the order in which voters voted).

Evaluation of an election system requires recognizing that some threats exist that must be protected against (e.g., poll workers who refuse to allow members of a given ethnic group to vote), some that cannot be protected against (e.g., a meteor strike on a polling place), and many that can be protected against if the Division of Elections, the legislature, and the public deem the cost of the protective measures worth the level of protection provided in return.

3.2 Assets

There are two major assets that are being protected in the current Alaska election system. These are the integrity of votes themselves and the public's confidence in the voting system. With regard to the votes themselves, the following items must be ensured:

- Each individual vote accurately reflects the intent of the voter who cast it.
- *Only* authorized voters can cast a vote.
- *All* authorized voters can cast a vote.
- The confidentiality of each vote is preserved (e.g., no one can determine how a particular voter voted).
- The integrity of each vote is preserved (e.g., the vote cannot be changed once it has been cast).

- The integrity of the result is preserved (i.e., that the final reported result is an accurate total of the votes cast).
- Votes are reliably categorized as valid or invalid (e.g., a ballot with two votes in a particular "choose-one" race should always be considered invalid).
- Data access, such as reads and writes of system data like ballot definitions, or modifications to system configurations (e.g., changes in the phone number used to send ballot data to a central computer) is limited to authorized participants.
- Data access and system management events are reliably attributed to an individual participant or component.

As we noted earlier, the public's confidence in the voting system is of primary interest in the evaluation of a voting system. While it is important that the voting system provides an acceptably accurate reflection of the voters' intent, it is also vital that the public believes in the system. For example, if the results reported on election night show Alice to be the winner and that result is overturned (quite possibly correctly) after an analysis of the paper ballots a week later, the public's confidence in the voting system is likely to suffer. Simply getting the correct result is not sufficient; it must also be demonstrated how and why the result was produced. The value of elections that are both trustworthy and perceived to be trustworthy is extremely high and, therefore the value of the electoral assets is extremely high.

3.3 Trust

In the election system, trust is placed in people and components.

People: How much trust is placed in the various people involved in the election process, from the voters themselves to the election system administrators? To what extent is this trust appropriately placed? What are the implications for the system, if a trusted person chooses to violate this trust? What are the methods used to examine, prevent, detect, and recover from violations of the system by trusted participants?

Components: It is vital to identify which components of the system (equipment and procedures) are trusted, the extent to which they are trusted, and the implications for the system if that trust is misplaced. For example, an optical scanning machine may be trusted to correctly count the ballots and accurately report the total votes cast for each candidate. However, how would the results be affected if the machine failed to count accurately?

In addition to identifying where trust is placed, the processes must take into account how trust is established. For example, how are poll workers selected and trained? How are the machines tested to ensure they function as designed? How is the design of the machines verified to ensure that it meets the specified functional and security requirements?

3.4 Deployment Environment

Election security studies have typically involved systems deployed in states with different procedural implementations and differing levels of authority to adopt processes and manage resources. As a result of these unique environments, it was not possible for these studies to fully address the extent to which vulnerabilities discovered in the components of the election system were mitigated or exacerbated by policies and procedures. Alaska's election environment is far more homogeneous, with a central entity (the Division of Elections) defining policies and procedures for state and federal elections across Alaska. Although the process is not exactly the same for all polling places in Alaska (particularly between urban and rural areas), there are many similarities that allow us to look broadly at the effects of policy and procedure on technical vulnerabilities in system components.

3.5 Adversaries

It is vital that the resources available to potential attackers not be underestimated. When identifying vulnerabilities in the election system as part of this project, we will attempt to describe any prerequisite information, access, or equipment that successful attackers must have—and assume they will be able to get what they need. Likewise, we'll assume that the system must be resilient against attacks by highly motivated and skilled people willing to commit significant time, money, and personnel to compromising an election.

3.6 Voting System Standards

The U.S. Election Assistance Commission was established by the Help America Vote Act of 2002 (HAVA). The commission is independent and bipartisan and is charged with developing guidance to help states meet HAVA requirements. It provides voluntary voting system guidelines and serves as a national clearinghouse of information about election administration. The commission also accredits testing laboratories and certifies voting systems, as well as audits the use of HAVA funds.

The 2002 Voting System Standard (United States Federal Election Commission 2002) is the current standard to which the voting systems in Alaska are certified, and that does address security to some extent. We used the 2002 standard as the basis for the definition of the term "secure" in this project.

There is a 2005 Voting System Standard, and the commission is currently considering the next iteration of the Voluntary Voting System Guidelines. Those address security issues in more depth than the 2002 standard, but no election systems had been certified against these new standards as of late 2007.

4 Alaska’s Election Processes, Procedures and Training

It’s important to know what Alaska’s current election system looks like, before we talk about how it compares with systems in other states and about potential security issues. We discuss the technology used in the system in more detail elsewhere, but at this point it’s helpful to summarize what equipment Alaska uses:

Global Election Management Systems (GEMS®): a server that runs election systems software and executes various election related tasks in combination with the AccuVote®-TSX and the AccuVote®-OS systems. The firmware version for GEMS® is 1.18.24.0. Five of these systems are used in Alaska at the regional and state-wide level.
AccuVote®-TSX , a touch-screen direct recording electronic (DRE) voting terminal, comprised of Ballot Station Version 4.6.4, Bootloader Version BLR 7-1.2.1, and Vote Card Encoder 1.3.2. There are 439 of these systems used in Alaska, one at each voting precinct, primarily for voters with disabilities that make it difficult for them to mark standard paper ballots.
AccuVote®-OS, a precinct and central accumulation optical scan voting system, version 1.96.6, and AccuFeed Device (paper ballot feeder). These systems are used in 290 precincts across Alaska. The remaining precincts conduct a hand count of their paper ballots.

4.1 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 4.1.1 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 4.1.2); the general dispersion and return of the optical scan voting machines (Sec. 4.1.3) and touch screen voting machines (Sec. 4.1.4) 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.

4.1.1 Icons Used in the Voting Process Diagrams

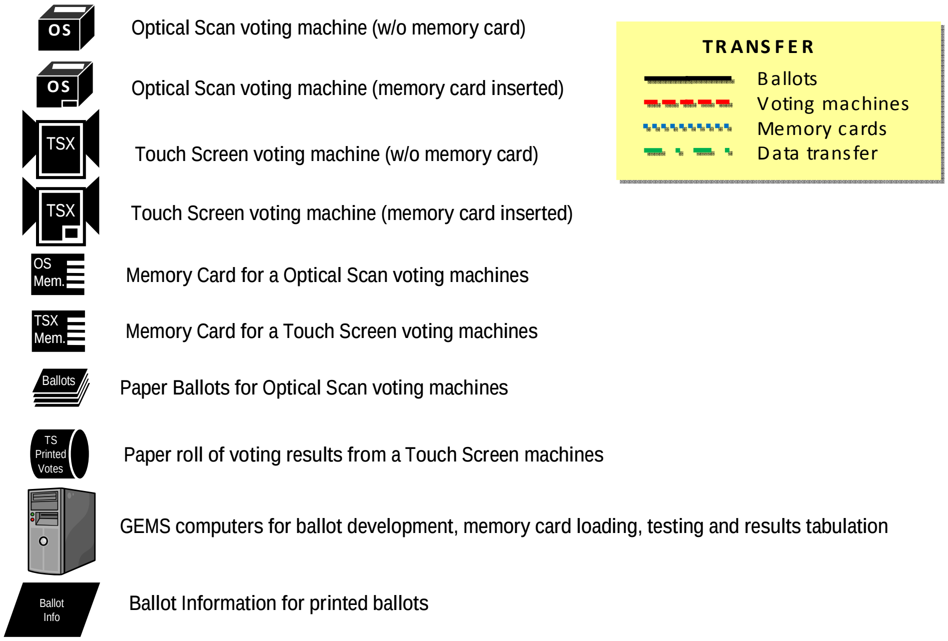

OS
Optical Scan voting machine (w/o memory card)
OS
Optical Scan voting machine (memory card inserted)
TSX
Touch Screen voting machine (w/o memory card)
TSX
Touch Screen voting machine (memory card inserted)
OS Mem.
Memory Card for a Optical Scan voting machines
TSX Mem.
Memory Card for a Touch Screen voting machines
Ballots
Paper Ballots for Optical Scan voting machines
TS Printed Votes
Paper roll of voting results from a Touch Screen machines
GEMS computers for ballot development, memory card loading, testing and results tabulation
Ballot Info
Ballot Information for printed ballots
TRANSFER
Ballots
Voting machines
Memory cards
Data transfer

Figure 3 - Voting Process Diagram Icons

4.1.2 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.

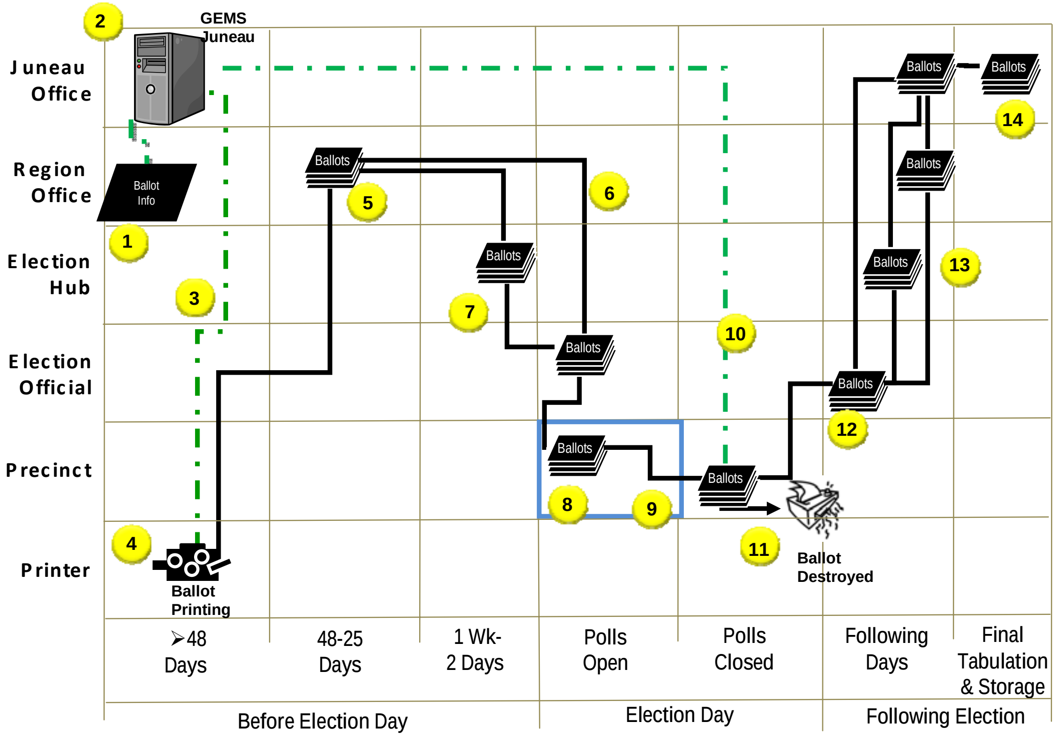


Figure 4 - Optical Scan Ballots and Hand-count Ballots – Chain of Possession

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 are called into Juneau.

11. The unused ballots are destroyed.

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

13. 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.

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

4.1.3 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.

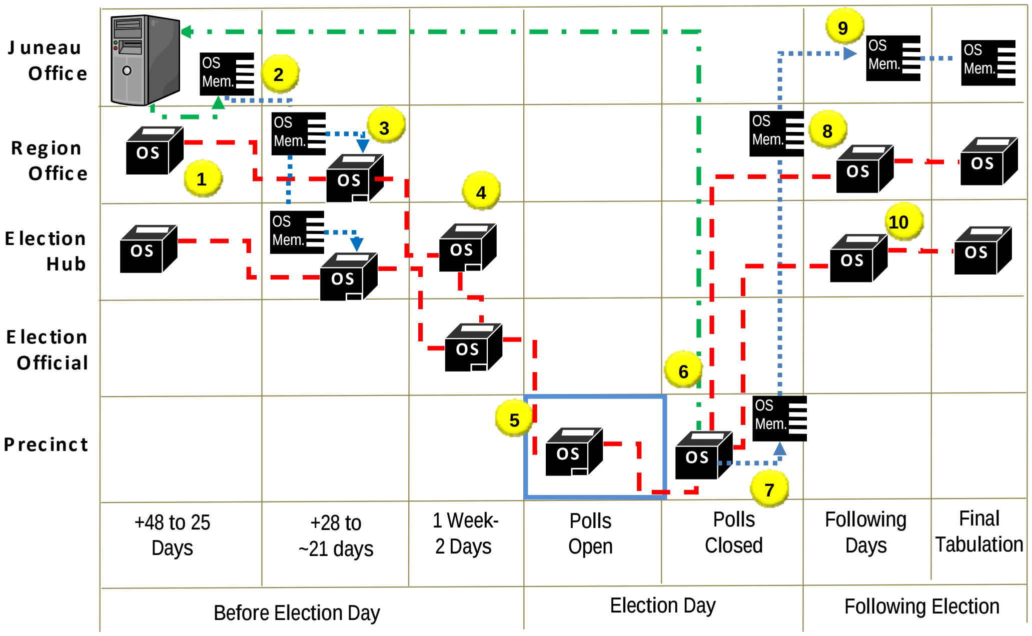


Figure 5 - Optical Scan Machine (OS) & Memory Card – Chain of Possession

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. 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.

4.1.4 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.

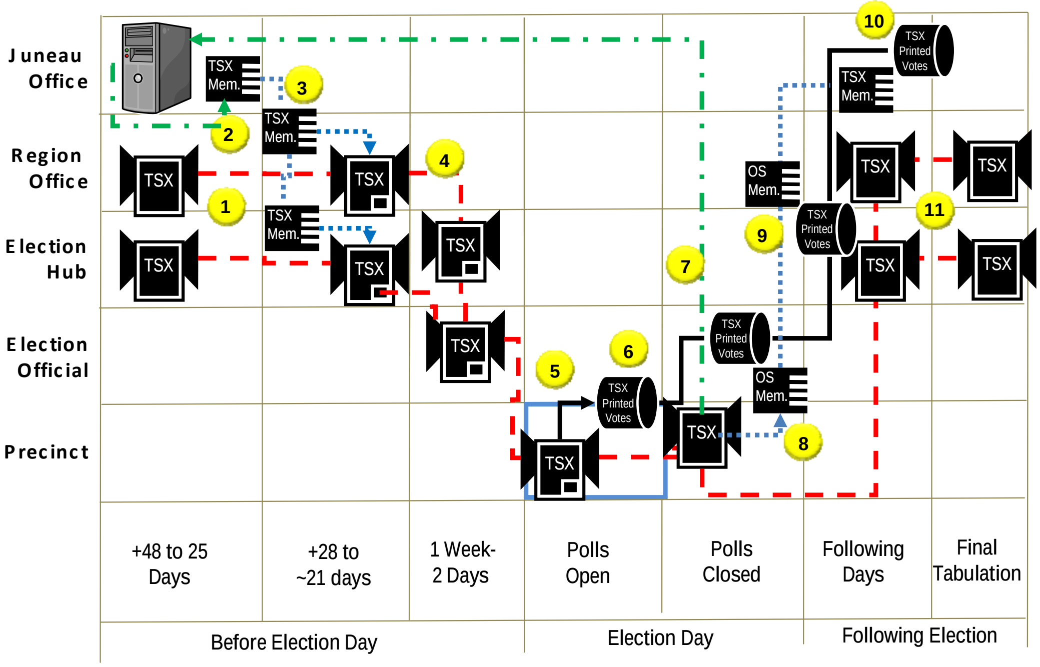


Figure 6 - Touch Screen (TSX) Voting Machine & Memory Card – Chain of Possession

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 TSX machine.

7. After the polls are closed, the final results are both printed from the TSX machine and the results are transmitted electronically to GEMS in Juneau.
8. The memory card, printed ballots, printed results summary are removed after the polls are closed and the TSX machine's results are transmitted.
9. The 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 TSX ballots rolls are returned to Juneau for review and, in the case of the ballot rolls, archiving.
11. The 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.

4.2 People and Training

Staffing of elections is determined by Alaska Statutes 15.10.105–15.10.180 (State of Alaska 2006). The lieutenant governor supervises the Division of Elections. The lieutenant governor appoints the director of elections. The director appoints a bi-partisan four person state ballot counting review board. The director also appoints election supervisors in each of the four regions (Juneau, Anchorage, Fairbanks, and Nome). Each regional election supervisor appoints a bi-partisan election board and a supervisor for each precinct in their district. The precinct election board appoints a bi-partisan team of four vote counters (subject to need in that precinct). Each political party, candidate not representing a political party, organization or group sponsoring or opposing an initiative may appoint observers for precincts or counting centers. Observers are allowed full view of the voting or counting from the time the polls open to when the results are certified.

Election officials have extensive access to voting equipment before, during, and after elections, and are keys to mitigating threats. Election officials also subscribe to an oath to be honest, faithful, impartial, and prompt in carrying out their election duties. All election officials are paid. The division of elections provides training programs before every state and federal election (every two years). Full-time election officials and temporary staff receive training. Election officials have suggested that we review procedures determining who has access to voting system components and evaluate whether they need to increase scrutiny.

4.3 Processes and Procedures

Compared with states that rely solely on electronics, Alaska has many processes and procedures in place that if implemented as written, add a layer of security to the electronic election system. These include:

- an election system that has paper ballots as a record of votes
- using machine counts and a sample of hand-counts to certify results
- a system of cross checks in vote counting that involves sending ballots and mechanical counting devices to separate locations after polls close
- an open election process that by statute includes observers.

In Alaska, a history of close elections has meant frequent re-counts and many opportunities to improve our counting procedures. Although not part of official processes, many of Alaska's election officials and precinct workers have long tenures with the Division of Elections and tremendous dedication to the election process. With the exception of the Director, who is appointed by the lieutenant governor, and the four regional supervisors, all employees of the Division of Elections are hired through the state personnel system and are not political appointees. This statutory change in the 1990s added another level of protection to the integrity of Alaska's system. In addition, Alaska has a small population and one voting system, so it is easier to have uniformity across the state and a built-in system of checks. Many of the recommendations for increasing security proposed for other states are already written into Alaska's state statutes and are part of the process here. Following the "Top-to-Bottom Review" (TTBR) of California's voting system, the California Secretary of State de-certified (then subsequently recertified) a voting system that is similar in many respects to Alaska's[3]. However Alaska's procedures around election day voting and vote counting are more comprehensive than those governing the handling of election equipment in the weeks leading up to elections.

How do the machines, people, ballots, and votes come together?[4] Voters can vote in several ways. Slightly more than 80% of voters cast paper ballots on election day, around 1% use touch screen devices, and the remainder (approximately 19%) participate in early voting or vote absentee by mail or fax. Because of time and resource constraints, this study does not cover early or absentee voting in Alaska.

After polls open, voters present identification, sign in on a registry, and receive a paper ballot. In larger communities the voter fills out the ballot, places it in a security envelope, and in view of an election official, slides the ballot into an optical scanner attached to a large ballot box. An optical scanner tallies the votes on the memory card. The paper ballot then slides into a locked ballot box below the scanner. In hand-count precincts, voters place their ballots directly into a locked ballot box.

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

[4] Voting and vote counting procedures are written into Alaska state statute AS15.15.195 to 15.15.480.

The other way to vote in a polling place is to use a touch screen device. The voter checks in at the polling place and is given a voter access card. The voter or polling place worker inserts the card into the touch screen machine. Touch screen devices work like bank ATMs. Voters choose from on-screen options, including language options and audio. An electronic copy of votes is stored in the machine. The machine also generates a paper record of the vote before the voting is complete, so that a voter can verify his vote. The voter can see the paper copy through a plastic screen but cannot take it with him.

According to federal law, election ballots for federal elections are archived in secure storage for 22 months. Defeated candidates or 10 qualified voters may apply for a recount of a precinct, house district or office. Since Alaska began using optical scanning technology in 1998, every state and federal recount has reaffirmed the accuracy of the original election results. After the polling place closes, the election board prints two copies of the results from the optical scanner. Each election worker signs both copies. Election workers remove the touch screen ballot tape. Election workers complete a ballot statement containing the number of ballots received, the number of ballots voted, the number of spoiled ballots, and the number of unused ballots. Unused ballots are either destroyed or returned to the district supervisor. In precincts using optical scanners, the election board connects the OS to unit a phone line and uploads the results to the GEMS computer in the director's office[5]. In hand count precincts, the election board counts votes in such a way that observers can see each ballot opened, read and tallied. The election board phones in results to the regional office and this becomes the unofficial election night result.

All precincts prepare two packages, dividing the electronic and paper records of the tallies so they can be checked against each other. The first package contains the memory card from the optical scanner, one copy of results, one copy of the touch screen results tape, and the ballots. In hand count precincts the first package contains one copy of the results, the memory card from the touch screen, the tally books, and ballots. The first package is delivered to the regional office or hub or mailed to Juneau[6]. The second package contains the second copy of the results, the voter registry and the ballot statement. Precinct boards send the second package directly to Juneau.

Election night, as results are either transmitted via the memory cards or hand-entered in the regional GEMS servers and uploaded to Juneau, they are posted as "unofficial." Within a day or two of the election, the regional supervisor sends the package they received from precincts—ballots, paper copies of the results and memory cards—to Juneau via chain-of-custody Alaska Airlines Goldstreak, DHL, or FedEx.

[5] In cases where election results cannot be directly uploaded: If the polling place is road linked to a hub or regional office, the election officer takes the card out of the OS and drives it to the regional office to be uploaded. (Results have already been printed). If the polling place is off the road system, the election supervisor calls in results to regional office where results are keyed in by hand.

[6] If the precinct is road connected to a regional office, the board delivers the first package to the regional office. If the precinct is not road connected to its regional office, but is connected to a hub, the precinct election board delivers the first package to the hub where they are sent chain-of-custody to Juneau. If the precinct is not road connected to a hub or its regional center, the precinct board sends the first package via business reply mail directly to Juneau.

The State Review Board in Juneau compares the results on the ballot statement with the memory card results. Once all of the ballots are in Juneau,[7] the state ballot counting review board begins its review and hand count verification process. Observers may attend the hand count verification. The State Review Board randomly selects one precinct from each of the 40 house districts, and the board hand counts ballots from that precinct. In order to be eligible for selection, the precinct must account for at least 5% ballots cast of the population in the house district. If the results from the hand count for a precinct differ from the optical scanner results by more than 1%, then the ballots for the entire district will be hand counted. After the hand counts, the director of elections certifies the election and results become official. In Alaska state and federal elections, totals from random hand-counts have always shown less than a 1% discrepancy from electronic tabulations

[7] This may begin as soon as practicable, but not more than 16 days after the election (AS15.15.440) when all absentee ballots are due.

5 Alaska Compared with Other States

How does the Alaska system we've just described compare with systems in other states? Each state can set its own election processes and procedures in conformance with requirements of the Federal Election Commission. These approaches can vary significantly.

In California, each county can establish its own processes and procedures. And in California a high percentage of votes are cast on touch-screen voting machines, and the election equipment is provided by multiple vendors.

In Florida, each county elects an election supervisor. Though the election code is uniform across the state, counties can choose from a selection of certified systems, including those used in Alaska. After the election in the year 2000, fifteen counties in Florida converted from punch-card based voting systems to to touch screen terminals for their primary voting systems. However, in advance of the primary elections in August 2008, all counties in Florida will be required to convert to optical scanning machines for primary vote tabulation. Until 2012, touch screen systems can be used to meet HAVA requirements. After 2012, Florida will phase out touch screen machines completely in response to security concerns of advocacy groups across the state. After 2012, paper-based "auto-mark" systems will be used to meet requirements for voters with disabilities. [Phone interview with Acting Director Sarah Jane Bradshaw]]

In Connecticut, elections are managed by 169 municipalities. Each municipality uses Premier AccuVote-OS systems and GEMS servers for primary vote tabulation. No touch screen systems are used. Once election results are tabulated at the municipal level, they are faxed the state-level office for final aggregation. To meet requirements for voters with disabilities, Connecticut uses IVS-Vote by Phone systems. Special stations are provided in each precinct to allow voters to cast votes using phone-based systems with specialized audio and visual characteristics. Once a voter submits a ballot, the system faxes back a record which the voter can verify (by listening or looking). This faxed copy of the ballot is then hand-counted by election officials at the municipality. Connecticut plans to use these systems through 2008. Each year, election officials will evaluate new technologies and determine if other, more beneficial systems should replace existing systems [Phone conversation with Leslie Mara, Deputy Secretary of State].

In Alaska, processes and procedures are centralized at the state level. Also, less than 1% of votes are cast on touch-screen machines. Alaska's election equipment is provided by a single vendor (Premier Election Solutions). The paper ballot remains the official ballot in Alaska. However, given Alaska's geographic diversity, transportation logistics and storage of election equipment can present some unique challenges not faced by other states.

Despite the many differences in approaches to election processes, one element common to Alaska, California, Florida, and Connecticut is the use of election equipment provided by Premier Election Solutions (formally Diebold). It is important to understand the differences in the how these systems are used in each state and how the processes and procedures affect election security in the context of the various state election systems. Figure 7 on the next page illustrates some of the unique attributes and similarities of election systems in Alaska, California, Florida, and Connecticut.

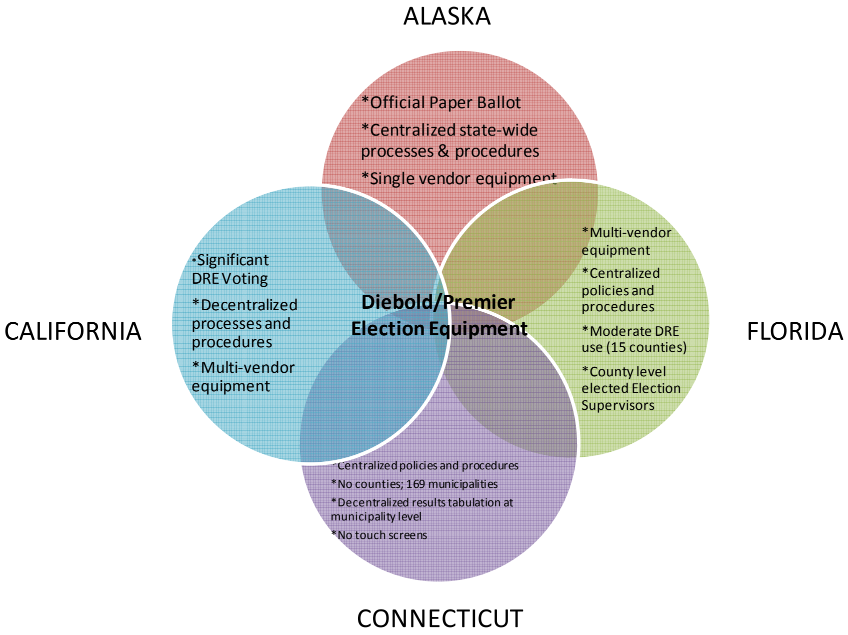

ALASKA
*Official Paper Ballot
*Centralized state-wide processes & procedures
*Single vendor equipment
CALIFORNIA
·Significant DRE Voting
*Decentralized processes and procedures
*Multi-vendor equipment
Diebold/Premier Election Equipment
FLORIDA
*Multi-vendor equipment
*Centralized policies and procedures
*Moderate DRE use (15 counties)
*County level elected Election Supervisors
*Centralized policies and procedures
*No counties; 169 municipalities
*Decentralized results tabulation at municipality level
*No touch screens
CONNECTICUT

Figure 7 - Alaska Compared with Other States.

6 Chronology of Studies

Since 2003, many studies have been conducted to evaluate Diebold election systems. To get a more complete understanding of the research that has been conducted and its potential applicability to Alaska, the project team reviewed a range of studies conducted in the past several years.

Early research conducted by Maryland, Ohio and other states was a catalyst for many of the more recent studies. In particular, studies conducted in late 2006 and throughout 2007 in California, Florida and Connecticut built a solid foundation for the Alaska team's evaluation. As these reports became public, Alaska's Lt. Governor Parnell sought to understand the potential implications for Alaska.

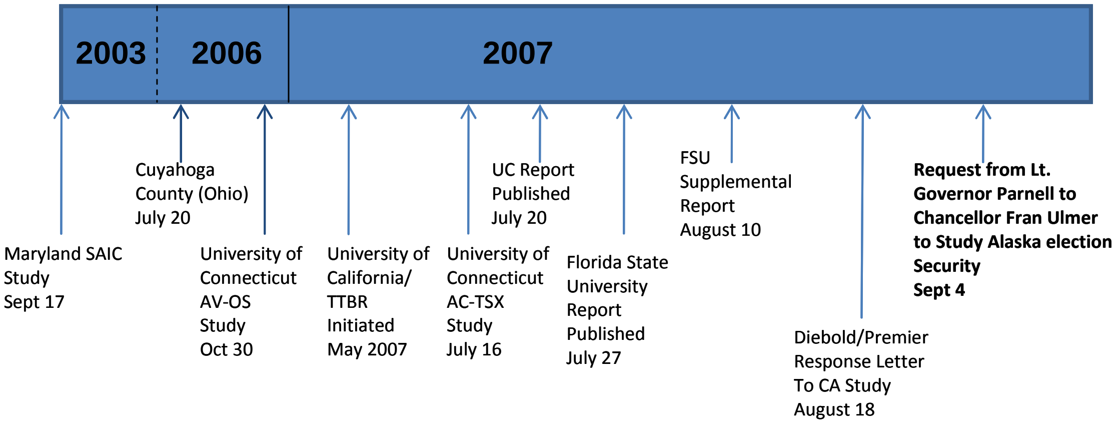

2003
2006
2007
Maryland SAIC Study Sept 17
Cuyahoga County (Ohio) July 20
University of Connecticut AV-OS Study Oct 30
University of California/ TTBR Initiated May 2007
University of Connecticut AC-TSX Study July 16
UC Report Published July 20
Florida State University Report Published July 27
FSU Supplemental Report August 10
Diebold/Premier Response Letter To CA Study August 18
Request from Lt. Governor Parnell to Chancellor Fran Ulmer to Study Alaska election Security Sept 4

Figure 8 – Chronology of Studies.

7 Technical Overview

7.1 Information Sources

In preparing this technical overview for Phase 1 of the Alaska Election Security Project, we consulted several sources, including the following two major recent election system security analyses:

- California's *Top-to-Bottom-Review* (TTBR): This project was conducted for the State of California during 2007 by leading academic security researchers and commercial security consultants. The goal was to complete a comprehensive security analysis of the election system in California, including a review of the various electronic voting systems at operational and source code levels.

- Florida's *Software review and security analysis of the Diebold voting machine software* and *Supplemental Report:* This project was conducted for the Florida Department of State and was led by the Florida State University (FSU) Security and Assurance in Information Technology (SAIT) Laboratory, in collaboration with nationally recognized security researchers. The project consisted of a source code review of several versions of the Premier Election Solutions (formally Diebold) software and systems, including versions more current than in use in Alaska. The initial work was followed by at least one additional review of software produced by Premier Elections Solutions in response to the findings.

In addition to the California and Florida reports, members of the Alaska technical team reviewed reports from Cuyahoga County in Ohio; Maryland; and the University of Connecticut. We also considered academic papers from the Institute of Electrical and Electronics Engineering, Inc. (IEEE), the Association for Computing Machinery (ACM), and other technical resources to identify potentially pertinent issues.

At the request of the technical team, Premier Election Solutions provided its written response to the California TTBR and a documentation CD containing user and administrator documentation for the AccuVote-OS Optical Scan, AccuVote-TSX Touch Screen, and GEMS server systems.

The Alaska Division of Elections was an excellent source of information throughout Phase 1 of the project. Shelly Growden, the HAVA Election Systems Manager for the Alaska Division of Elections, hosted the evaluation team at the Fairbanks regional office on multiple occasions. During these meetings, she provided detailed descriptions of the election processes in Alaska. These sessions also gave team members an opportunity to gain hands-on experience with the operation of the various devices used to manage and run elections in Alaska. Ms. Growden also provided valuable insight into the perceived security strengths and weaknesses of the current Alaska equipment and processes. She described the additional steps the Alaska Division of Elections has already undertaken to address some vulnerabilities identified internally in the Division of Elections. Whitney Brewster, the director of the Division of Elections, Carol Thompson, Absentee and Petition Manager, and Denali Elmore, Election Supervisor Region 2 (Anchorage and Mat-Su), hosted members of the research team in Anchorage for a subsequent hands-on session.

Kevin Keelan of SysTest Labs, Inc. provided an overview description of the voting systems' testing conducted by his company. SysTest Labs is an accredited voting system Independent Testing Authority (ITA) which performs the required hardware, software, and documentation review as part of the U.S. Election Assistance Commission (EAC) voting system certification process

Kathy Rogers, Jeffrey Hallmark, and Talbot Iredale from Premier Election Systems provided information detailing software and firmware revisions made to their systems subsequent to the California and Florida studies. They also provided a status report for their submittal of these changes for VSS 2002 certification. According to their statements at the time of this report, the test plan for these changes is under review by the Election Assistance Commission.

7.2 System Configuration

The State of Alaska currently uses Premier Election Solutions (formerly Diebold) hardware and software in its election system. The equipment includes GEMS (Global Election Management Systems) servers located in Juneau and the regional Division of Election offices, Premier AccuVote-OS Optical Scan (in selected precincts), and AccuVote-TSX Touch Screen voting machines in each precinct. The hardware and software used is the most recent version certified against the 2002 Voting System Standard. As described above, Premier has produced more recent versions of these components which have been submitted for VSS 2002 certification by the Election Assistance Commission. However, at the time of this report these changes have not been certified. The following versions of these components are currently in use in Alaska:

- AccuVote-OS Optical Scan, firmware version 1.96.6
- AccuVote-TSX Touch Screen, firmware version 4.6.4
- Diebold Touch Screen bootloader version 1.2.1
- GEMS server software version 1.18.24.0

Figure 9 shows a diagram of the election machines used in the Alaska system. The GEMS server is used to program memory cards that are distributed to the regional offices in advance of the election. On Election Day, voters cast votes by either filling out a paper ballot, which is then counted by an AccuVote-OS Optical Scan machine, or by using the AccuVote-TSX Touch Screen device, which creates and retains a voter verifiable paper trail (VVPT) that serves as the official ballot.

When the polls close on Election Day, the vote totals stored on the memory card in each machine are reported to the GEMS server using a modem connection through a phone line (where possible). The paper ballots and audit logs are returned to the Division of Elections hubs or regional offices following the election and later sent to the Division of Election in Juneau.

The electronic totals are tallied and reported on election night as unofficial results. The results are considered to be official when a bi-partisan State Ballot Review Board reviews materials from each precinct and conducts a manual recount of no less than 5% of the paper ballots from randomly selected precincts. These totals are compared with the unofficial electronic totals tabulated on election night. If the totals do not match, a mandatory hand-count of the paper ballots for the entire district is ordered.

This GEMS server in Juneau is the beginning point for state and federal elections.   It is programmed to include information from candidates, numbers of registered voters in each precinct, and other election information. Once this information is programmed into the central GEMS server it is used to program the individual memory cards used in AV-OS and AV-TSX systems distributed from the regional offices. After the polls close, “unofficial” election results are compiled by the central server in Juneau based on results tabulated at and transmitted by the regional offices.   After the election, the memory cards, ballots and other election material are returned to Juneau where it is validated and archived in keeping with federal and state election policies. The following diagram is a simplified representation of this process.

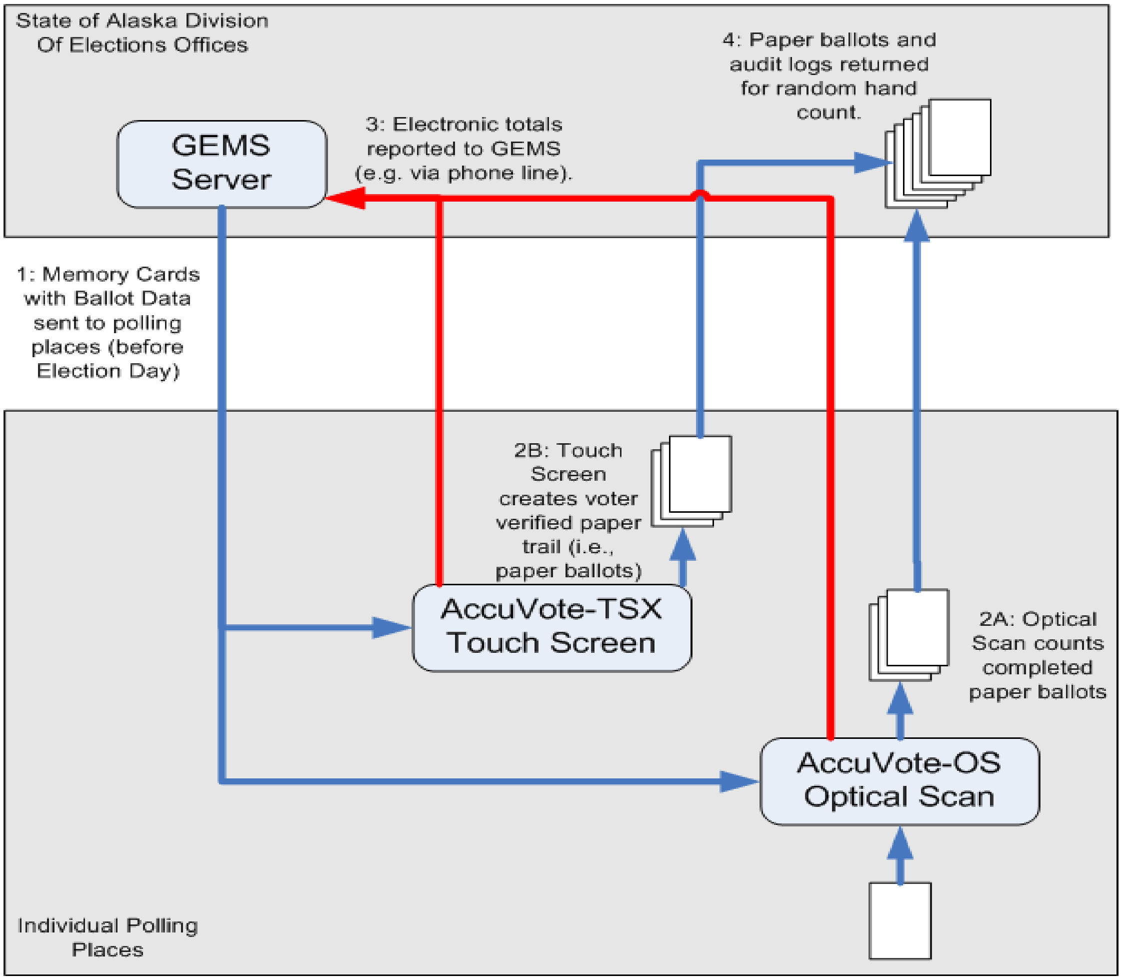

State of Alaska Division Of Elections Offices
4: Paper ballots and audit logs returned for random hand count.
GEMS Server
3: Electronic totals reported to GEMS (e.g. via phone line).
1: Memory Cards with Ballot Data sent to polling places (before Election Day)
2B: Touch Screen creates voter verified paper trail (i.e., paper ballots)
AccuVote-TSX Touch Screen
2A: Optical Scan counts completed paper ballots
AccuVote-OS Optical Scan
Individual Polling Places

Figure 9 - A simplified view of the components of the Alaska election system, and the data flow between them. A more detailed description of this process is in Section 4.

8 Overview of Studies

8.1 State of Maryland Reports

In 2003 the State of Maryland contracted with Science Applications International Corporation (SAIC) to assess security risks for the Diebold AccuVote-TS electronic voting system (State of Maryland, 2003). SAIC performed its assessment between August 5 and August 26 of 2003. As part of its report, SAIC addressed security vulnerabilities brought up by Aviel D. Rubin in what is known as the “Hopkins Study” or “Rubin Report.” This report was published in 2004 (Kohno et al., 2004). In November 2003 Maryland contracted with RABA Technologies, LLC to examine and critique the findings of both the SAIC and Hopkins reports (RABA Technologies, 2004). All three studies agree that vulnerabilities exist and that if exploited could significantly affect the accuracy, integrity, and availability of Maryland’s election results.

8.1.1 Hopkins Study

The Hopkins report reviewed the source code for the AccuVote-TS electronic voting system and found several significant vulnerabilities, including flaws that allow a malicious voter with a forged smartcard to vote multiple times or access administrator functions. Other flaws include weak techniques for key management and encryption;potential ways of linking voters to votes or tampering with election results; buffer overflow errors; and inconsistent and sometimes sloppy coding practices. Later studies (see section 8.5) report that some, but not all, these flaws have been corrected.

8.1.2 SAIC Study

The SAIC study reviewed Maryland’s voting requirements, procedures, and plans in addition to a technical evaluation that included an assessment of the Hopkins report. It criticized the state’s lack of a formal, documented, system security plan with explicit requirements, a process to ensure the integrity of the voting system, appropriate access controls to servers and equipment, and a process to detect unauthorized access attempts. Moreover, the State Board of Elections did not require secure transmission of vote totals, review audit trails, or provide training for election personnel that includes a component on information security.

On the technical evaluation, the SAIC study agreed with some of the findings from the Hopkins study but dismissed others as not applicable or low-risk. For example, flaws in the network code were dismissed because Maryland did not connect its machines to a network. Similarly, exploits that require physical manipulation of the machine (e.g., opening the lock and tampering with the card reader) are discounted because limited privacy in the voting booth would allow an election official to detect such activity.

8.1.3 RABA Study

The RABA study agreed with the Hopkins report on technical matters but criticized it for failing to discuss other mitigating controls. Alternately, the RABA study criticized the SAIC report for dismissing vulnerabilities covered by a separate control, such as discounting the possibility that a malicious voter might insert a forged smartcard because a watchful election official would detect such tampering. Instead, the study said a layered approach or "defense in depth" should be employed, with the assumption that precautions and systems may fail but the system is still able to recover.

The RABA report concluded with an exercise in which researchers were able to exploit several vulnerabilities to access the contents of smartcards and change voter cards into administrator or security key cards. Additionally, the team was able to pick the locks on the machines in 10 to 60 seconds, giving them physical access to disrupt the machine or perform administrator functions. Finally, the team was able to hack into the GEMS server, given physical or network access. To mitigate these vulnerabilities the recommended the use of tamper tape, computer-generated passwords by precinct, alarms on the bay doors, lockdown of the GEMS server, and the use of auditing tools.

8.2 Cuyohoga County of Ohio Election Review Panel Report

Cuyahoga County in Ohio commissioned a review of its electronic voting process using AccuVote Optical Scan (AV-OS) equipment. The report is extensive, covering almost 400 pages, but focuses mostly on management issues related to poor planning, poorly written contract language, and unsatisfactory logistics. Among the findings are a large number of malfunctioning AV-OS units, limited voter privacy (due to poor placing of the equipment), concerns regarding the chain of custody, lack of training for the poll workers, and in general unsafe and error-prone practices. Among the fixes, the report recommends parallel testing, done not only in test mode but also in election mode, during the election process. Additionally, the report recommends the use of numbered seals, with repeated checks of the integrity and of the serial number of the seals, possibly using bar codes for speed.

Appendix M in the Ohio review is a report from SysTest Labs, LLC, focused more on the technical vulnerabilities of the system. Many of the errors reported were the result of a poor design of the ballot, which placed some of the voting ovals too close to the separator lines on the paper. Due to limited precision in scanning, the separator lines were often counted as valid votes. One of the machines tested with blank ballots had an error rate of 45%. Additional issues identified were the lack of an error message when the memory card became full (the system just stopped counting votes, or overwrote existing votes), and problems with the GEMS audit log (attempts to vote with an invalid ballot were not logged).

The issues identified as most troubling were lack of training of workers, concerns with the storage space for the voting equipment (in a room with a wet sprinkler system, which could potentially damage the equipment), lax security practices for access to the storage room, and limited security measures for protecting the equipment against tampering. As mentioned above, the study recommended the use of custom numbered security seals and the frequent tracking of the seal number and integrity (using bar codes for speed). The report also recommends better tracking and tamper-evident measures for the materials boxes, and for the elections supplies.

8.3 University of Connecticut Voting Technology Research Center Report

In a series of papers, a group from the Voting Technology Research Center (VoTeR Center) at the University of Connecticut, led by A. Kiayias, L. Michel, A. Russell, and A. A. Shvartsman, evaluated the vulnerabilities associated with the AccuVote Optical Scan (AV-OS) and AccuVote Touch Screen (AV-TSX) systems. The reports point out that once these vulnerabilities are well understood they might be mitigated or eliminated by carefully designed policies and procedures. All the reports recommend pre-election testing of memory cards, strict control over the chain of custody of the voting terminals and the memory cards, and post election audits (hand counts).

The reports also document attacks on the voting equipment. The attacks were conducted without access to any internal documentation or source code from the manufacturer or the vendor, but based only on the attackers' observation and knowledge of basic principles of hardware security. The attacks used off-the-shelf computing equipment, combined with reverse-engineered software. Given as little as 5 minutes, the authors demonstrate how they can pick the lock on the enclosure of the voting equipment, connect a laptop computer to the AV-OS, download the configuration, modify it, upload the modified version, and remove any trace of the attack. This last step involves tampering with the audit log of the equipment, disabling the audit tape printer and restoring the original timestamp on the configuration software.

The modified voting configuration allows the attackers to swap votes for two candidates or to make votes for one candidate not count at all. Moreover, the investigation showed how it is possible to make the equipment work correctly for the first few ballots or to operate correctly for any ballots before Election Day--so the voting equipment will appear to operate correctly for the initial testing and will switch to the rigged configuration to count the actual ballots.

Gaining access to the configuration software is facilitated by the lack of authentication in the AV-OS system. The attack can be conducted using the serial port or the modem port, after picking the lock of the enclosure of the equipment. Picking the lock can be done with two paper clips and moderate lock-picking skills, because the locks are standard for most office equipment. As such, tamper evident seals are recommended for the enclosure, with numbered seals verified at multiple points along the election process. Additionally, the investigators recommend disconnecting internally the serial port and the modem port, although this has limited potential to prevent access to the software. The report also recommends placing the voting equipment in a place that can ensure privacy for the voting process, but not sufficient privacy to conduct an attack as described.

Additionally, a strict chain-of -custody, checks and audits of the memory cards are recommended, as well as of the firmware chip. The firmware chip is removable to allow version upgrades, and election officials need to ensure that the existing chip is of the right version. The verified chain of custody by itself is not sufficient to protect the integrity of the software, as demonstrated by the attacks above.

Finally, the AV-OS is vulnerable to an even more basic attack, which allows an attacker to vote multiple times, by holding on to the ballot with two Post-It® notes. The Post-It® notes allow the attacker to retrieve the ballot after it is scanned and fed into the box. AV-OS does not prevent ballots from being extracted this way, and does not have any means to recognize that a certain ballot has already been counted.

All of the attacks above can be detected and corrected for the AV-OS by a hand count of the ballots in the box. As such, post-election audits are essential to ensure correct results.

In a paper reviewing an AV-TSX system (firmware 4.6.4, bootloader BLR7-1.2.1 using Windows CE version WCER7-410.2.1, using GEMS 1.18), the same UConn investigators report on the same two types of attacks: one that effectively removes a candidate and one that swaps votes for two candidates. The first attack is possible because of a design flaw in the system. Each candidate entry in a configuration file is accompanied by a checksum, a number that verifies the validity of the entry. If this checksum is corrupted, the system should not operate and should give an error message. Instead, if the checksum is corrupted the equipment still operates, but the votes for the candidate are not counted. To effectively remove a candidate, an attacker only needs to tamper with the checksum to make it invalid. The second attack is also enabled by a design flaw. Two different configuration files control the order of the candidates on the display and the order of the candidates in the database with the vote count. By exchanging the placement of two candidates in the database file but not in the display file, the votes as displayed on the screen will be associated with different candidates in the database. The recommendations for protecting the AV-TS equipment are similar with those for the AV-OS, but the post-election audit is less trustworthy than for the voter-completed ballots of the AV-OS system.

8.4 State of California “Top-to-Bottom Review” (TTBR) Report

8.4.1 Introduction

We reviewed the technical studies that were part of California’s TTBR (Top-to-Bottom Review), an electronic voting system evaluation completed in July 2007. The California technical study included a source code analysis, a documentation review, an accessibility review and a red team review of the Diebold[8] AccuVote Touch Screen and AccuVote Optical Scan voting machines as well as the Diebold GEMS (Global Election Management System) server.

Alaska’s electronic voting system uses Diebold Global Election Management System, Accuvote Touchscreen, and Accuvote Optical Scan voting machines identical to those evaluated in the California TTBR report. Clearly Alaska has an interest in the relevance and impact of the results presented in the California report as they relate to Alaska’s electronic voting system. The ease with which the attacks identified in the California TTBR could be executed within Alaska’s system was not assessed as part of this report. These findings should be evaluated within the entire Alaska context, including existing processes and procedures, in a more in-depth Phase 2 evaluation.

8.4.2 State of California Source Code Report Summary

Alaska’s summary of the State of California Diebold TTBR voting system analysis consisted of two major technical components. These components were a source code review and a red team analysis. In

[8] The Diebold Company has changed its name to Premier since the California study was written. Since the California report makes all references to the company Diebold, this document will refer to the manufacturer as Diebold to avoid confusion.

addition, there were separate documentation and accessibility reviews. Neither a detailed summary of the documentation review nor the accessibility review is included in this report; however, both reports also identified several areas for concern that should be evaluated in a more detailed Phase 2 analysis. The California TTBR reports can be found in the Supplemental Documentation package distributed with this report.

The source code review of the Diebold system was focused primarily on the Diebold AccuVote-TSx (AV-TSx) touch screen and AccuVote-OS (AV-OS) optical scan system software along with the Diebold GEMS election management system software for design or implementation flaws. The red team's review of the Diebold system focused on identifying and attempting attacks on the Diebold system and documenting the success of those attacks. In all cases of the California TTBR source code and technical reviews, the vulnerabilities identified were of a technical nature and the ability of a malicious attacker to exploit these vulnerabilities was assumed and was not considered further.

Time and financial considerations led the State of California team to focus on several different high level questions in developing an analysis methodology for their TTBR. The questions posed were designed to determine whether effective safeguards were in place in the system provided. A summary of these questions is provided below.

- What are the trusted system components?
- Is the implementation of cryptography sound across the Diebold system?
- Can a system security failure be detected?
- Can the privileges of a user be escalated or compromised?
- Is the system design soundly engineered and implemented?
- Can the system be analyzed in a quantitative manner?

Using these questions as a guideline, the California review team analyzed the system and found several high level system vulnerabilities.

The technical vulnerabilities identified by the California technical review are as follows:

- Vulnerability to malicious software

  The Diebold system software was vulnerable to the installation of malicious software which could allow incorrect recording of votes, miscounting of votes or the prevention of voting machine operation.

- Susceptibility to viruses

  The Diebold voting system was found to be susceptible to computer virus infection which allowed voting machine to voting machine and voting machine to election management system virus propagation.

- Failure to protect ballot secrecy

  The Diebold AV-TSx touch screen system retains sufficient information in its memory to compromise the secrecy of ballots cast.

- Vulnerability to malicious insiders

  The Diebold system did not contain sufficient access and management control to ensure that authority clearances assigned were securely maintained.

- AV-TSx vulnerability of paper trail to tampering

  It was found that the paper trail produced by the AV-TSx machine was susceptible to tampering through the use of a common household substance. The vulnerability was found to be successful in destroying the paper trail of votes cast prior to and following the attack.

  GEMS system configuration security vulnerability

  The Diebold-provided GEMS system configuration was found to be insecure upon delivery. The California team found several system level vulnerabilities with the configuration of the GEMS server provided.

The source code review team found that the Diebold system suffered from systematic flaws which were a result of a system design in which security and secrecy were not primary objectives. These design flaws were found to be difficult to mitigate procedurally.

8.4.3 Diebold Response to California Source Code Review

In response to the report that was produced by the California team Diebold produced a document which referred to the major issues identified in that report. The Diebold response document is available from the California Secretary of State's Web site. The contents of the Diebold response were taken into consideration while this review was written.

8.4.4 Diebold System Hardware

A comparison of the system tested by the State of California with the system used by the State of Alaska shows that the system evaluated in California is identical to the system currently in use by the State of Alaska. All hardware, software and firmware versions currently used in the State of Alaska are identical to those that were evaluated in the California report.

The system analyzed by the California TTBR consisted of the following hardware:

Primary Diebold System Hardware

1. Diebold Global Election Management Systems (GEMS) Server.
   The GEMS server runs the election systems software and executes various election related tasks relevant to both the AV-TSx and AV-OS platforms. The GEMS server uses an off the shelf Windows Operating System and Microsoft's Jet database implementation.

   - Election Management Version 1.18.24.0

2. AccuVote Touchscreen Device (AV-TSx). The AV-TSx device operates as a direct recording electronic (DRE) voting terminal. Upon the casting of each ballot a paper audit

physical ballot is printed using an attached printer. This device relies on a PCMCIA memory card device which defines the election ballot and other polling details. The contents of this PCMCIA device are transferred to the GEMS system upon completion of the election.

- BallotStation Version 4.6.4
- Bootloader Version BLR 7-1.2.1

3. AccuVote Optical Scan Device (AV-OS). The AV-OS device gathers, stores and tallies optically scanned ballots which are fed by voters to the system. The AV-OS system relies on an Epson 40-pin memory card to store system configurations and election definitions. The contents of the memory card are transferred to the GEMS system upon completion of the election.

   - AccuVote-OS Precinct Count Version 1.96.6

In addition to the primary hardware, several other components are required to complete the Diebold system. These devices are listed below:

Secondary Diebold System Hardware

1. AccuVote Central Count AV-OS. This device is a standard AV-OS connected to the GEMS server at a central counting facility and is used to read bulk paper ballots.
   **Note: The State of Alaska does not use the AccuVote Central Count AV-OS in its implementation of the Diebold electronic voting system.*

2. AccuFeed Device. This device is used to feed paper ballots into an AccuVote Central Count AV-OS. (**Note: The State of Alaska does not use the AccuVote Central Count AV-OS in its implementation of the Diebold electronic voting system.)*

3. Smart Cards and Smart Card Reader. Smart cards are used by the Diebold AV-TSx system to control security and administration during the election process. A smart card is inserted into the AV-TSx device prior to voting or during system administration activities.

   - Key Card Tool Version 4.6.1 (**Note: The State of Alaska does not use the Key Card Tool in its implementation of the Diebold electronic voting system.)*
   - VC Programmer Version 4.6.1
   - Vote Card Encoder Version 1.3.2

8.4.5 Major Attacks

The California TTBR identified several major attack scenarios by which the voting system might be compromised. A summary of these attacks is provided below.

1. Voting Machine Viruses
   The review found that the AV-TSx and AV-OS devices are susceptible to viral software spreading through the insertion of infected memory cards. The viral infection introduced into the system has the potential to affect multiple election cycles if undetected. Infection of the AV-TSx or AV-OS system can be spread to the GEMS server during the vote counting

process. This type of secondary infection could result in significant system compromises. The AV-TSx platform was found to be more vulnerable than the AV-OS platform because it prints the voter-verifiable paper audit trail (VVPAT) as the ballots are cast. This allows a malicious programmer to affect both the electronic tally and the paper tally during the attack. Implementation of a viral attack on the system requires significant technical expertise.

It was further found that a viral infection spread from the GEMS server machine to individual AVTSx and AV-OS machines was also possible. This type of viral infection could be propagated by the distribution of memory cards during election administration.

Two major virus types were identified in the California report. In the first scenario, the viral software infection would be used to steal votes (by changing tallies or shifting votes) in a subtle manner. In the second scenario the virus software would be used to implement a massive denial of service attack.

Based on the tasks outlined in the California report, a viral attack on Alaska's system is also feasible. However, the ease with which the attacks identified in the California TTBR could be executed within the State of Alaska's system was not assessed as part of this report. Alaska's primary electronic voting platform is the AV-OS machine which was found to be less susceptible to viral attacks than the touch-screen AV-TSx devices.

2. Voter Verified Paper Audit Trail (VVPAT) and Ballot Secrecy Attacks

   The design and implementation of the AV-TSx VVPAT mechanism was found to pose a threat to the secrecy of voter ballots and to place a limit on the ability to detect malicious software. Several scenarios are presented in the California report surrounding techniques for compromising the VVPAT implementation of the AV-TSx device.

   The AV-TSx devices were found to have flaws which could compromise voter ballot secrecy. It was found that the AV-TSx machine stores the vote record with a time stamp which can be determined by compromising the system encryption. The California team found that the nature of the sequenced ballot preservation inherently reduced the secrecy of the votes cast.

   The State of Alaska utilizes the same AV-TSx machine as the California system to provide federally mandated HAVA (Help America Vote Act) access at polling places. The ease with which a motivated individual might execute a VVPAT attack within the State of Alaska system was not assessed as part of this report.

8.4.6 Systematic and Architectural Issues

The California team analyzed the Diebold election system to determine if systematic or architectural design issues were present which might compromise the system integrity. The team found that significant systematic weaknesses were present in the design, implementation and engineering practices which were used during the system development process.

The California TTBR contains a detailed discussion of the issues identified during their study. The State of Alaska uses identical hardware and software versions to those presented in the California report. A list of the issues is presented below. For a detailed discussion of each issue the reader is directed to the California Source Code Review and Red Team documents. The following paragraphs summarize the major systematic and architectural issues identified in the California reports.

1. Large Attack Surface
   It was found that the scale of the interfaces exposed to a potential attacker was large. The implication of this large "attack surface" is that significant vulnerabilities may exist and hence more attacks on the system are possible. The California technical review team noted that if more time were available, the red team would have likely identified more issues.

2. System Complexity
   The Diebold system was found to lack assurance. A typical goal in the design of secure systems is to state the desired functionality clearly and to achieve it using the simplest possible design and implementation in a manner that evaluators can verify meets the desired functionality. The Diebold system did not appear to be designed and implemented in this manner.

3. Misplaced Trust
   The software designed for use in the Diebold system was found to place too much trust in people and in communications between devices.

4. Bi-directional Information Flow
   The Diebold system uses data flow both from the GEMS to the field devices (AV-TSx and AS-OS) and from the field devices to the GEMS. This type of communication between devices provides an easier path for viral infection than in a system where only one direction of data flow is possible.

5. Code Integrity Controls Are Not Sufficient
   The AV-TSx and AV-OS devices do not provide strong controls on the integrity of the system software. The AV-TSx devices were found to be particularly susceptible to code integrity compromises. The AV-OS hardware was found to be more robust, but still susceptible to attacks when the attacker was physically present at the machines location.

6. Code Integrity Verification Not Possible
   The AV-TSx and AV-OS devices were found to have no provisions to allow an election official to verify that the version of firmware present on the device is the correct version for the election.

7. Reliance on Commercial Off The Shelf (COTS) Software
   The Diebold system utilizes COTS software for several components of the system implementation. The COTS software selected for use in the Diebold system increases the size of the system's "attack surface".

8. System Modems and Other Networks
   The Diebold system includes voice modems for communication between devices (AV-TSx and AV-OS to GEMS and Regional GEMS to Headquarters GEMS). Connection of these devices to a PSTN (Public Switched Telephone Network) exposes the devices to threats from

a large number of unknown sources. Several security issues were identified in the communications protocols and systems implemented by the Diebold engineers.

In addition to identifying systemic and architectural issues, the California team also identified implementation issues with the Diebold system.

1. Input Validation
   Consistent and disciplined input validation in the system software was not found in the Diebold system. A standard template for input validation was not apparent from the California team's study.

2. Defensive Programming
   Defensive programming methods used in the Diebold development were found to be variable and inconsistent. In some cases the software was found to be robust and defensive while in other cases it was found to be weakly defensive.

3. Programming Language Choice
   The Diebold system utilizes C, C++ and assembly programming languages in the software implementation. These languages are known to have security risks associated with memory management. The California report noted that more robust language choices exist for implementing secure systems.

During the process of conducting the study the California team made several observations regarding the engineering processes used during the development of the Diebold system. These observations are listed below.

1. No Formal Threat Model or Security Plan
   It was discovered (through an interview with Diebold's software development manager) that no formal threat model or security plan existed in the development model for Diebold's voting system. This discovery was found to be evident in the source code analyzed by the California team.

2. No Formal Security Training
   No specific security training or red-team testing procedures existed during the development process. It was discovered that although some of the software developers had security backgrounds, no specific security training was provided to the software developers.

3. Weak Source Code Review Process
   The source code review process was found to have significant holes and was not implemented in a robust manner which ensured reliable, valuable source code review was performed during the development process.

4. No Unit Testing or Red Team Testing
   Diebold did not develop or use any formal red team testing procedures during the system development. No formal requirement existed by which developers were responsible for providing tests to verify the validity of code being developed. As such the developed code was only checked using test procedures that may or may not identify potential security threats.

8.5 Florida Software Review and Security Analysis Summary

8.5.1 Introduction

The Florida Department of State commissioned the *Software Review and Security Analysis of the Diebold Voting Machine Software Study*, which was led by the FSU's Security and Assurance in Information Technology (SAIT) Laboratory. The resulting report describes the analysis of the following four election system components:

- Diebold AccuVote Optical Scan
- Diebold AccuVote Touch Screen
- Diebold AccuVote Touch Screen boot loader
- GEMS server software

The FSU team used a unique approach where potential adversaries were classed into role groups to help associate potential system flaws with the individuals who would be in a position to exploit the flaws. These classifications included:

1. Voters
2. Poll Workers
3. Election Officials
4. Voting System Vendors

The first two categories were considered in the investigation whereas the final two were considered to be outside the scope of the study. They also classified the skills required to mount attacks and made it clear that they were referring to the individual developing the exploit, as subsequent attackers could likely use the exploit once it had been developed without possessing a comparable technical skill level.

The initial objective was not to identify new flaws, but rather to compile a list of identified flaws from the current literature and determine the status of the associated vulnerabilities. 126 flaws were identified in previous versions of the Premier systems from the literature reviews, including the studies mentioned in previous sections. These flaws were each categorized into a matrix that identified the applicable component to which the vulnerability belonged. The investigators then sought to classify each vulnerability as either *No Change*, *Improved*, or *Fixed* based on analysis of the code in the most recent version of the software/hardware. The results indicated that while many flaws were no longer present in the latest version of the Premier systems, many more had not been adequately addressed and left the systems vulnerable to exploitation.

8.5.2 How does this compare with current Alaska systems?

The Florida study tested all of the components that are in use in Alaska, but more recent versions of the system software were tested. The specific versions tested are as follows:

- Diebold AccuVote Optical Scan, firmware version 1.96.8 (Alaska has version 1.96.6)
- Diebold AccuVote Touch Screen, firmware version 4.6.5 (Alaska has version 4.6.4)
- Diebold AccuVote Touch Screen bootloader, version 1.3.6 (Alaska has version 1.2.1)
- GEMS server software version 1.18.25 (Alaska has version 1.18.24.0)

One objective of the code review was to evaluate the new software that had been submitted for certification by the Florida Department of State. According to statements made by Premier Election Solutions, these changes have been submitted for VSS 2002 certification. The report made the following observations regarding the flaws reported in previous studies:

- 40 of the flaws identified in the original literature search have been fixed in the version tested in Florida.
- 31 of the flaws had been improved, although not completely fixed.
- 37 of the flaws remain unchanged.
- 18 of the flaws were not considered pertinent to this review.

Note that the Florida study did not make a recommendation in regard to the certification process, but rather presented findings to allow the Department of State to make an informed decision. In addition to the public documentation, two non-public appendices were produced, which contained Propriety Issues and Non-Pertinent Flaws identified during the study.

8.5.3 Florida Department of State Actions:

The Florida Department of State evaluated the findings and determined that many of the flaws were administrative in nature or posed no security risk, and issued technical advisories to election supervisors as the means to mitigate these flaws.

In addition, the Florida Department of State identified four corrections that had to be made in order for the optical scanner voting machines to be certified for use in Florida elections. These include the following:

- Signature Flaw (Optical Scan)
- Attacker can hide preloaded votes (7 associated flaws)
- AccuBasic Scripts Can Be Misused (4 associated flaws)
- Unchecked String Operation (2 associated flaws)

Based on the results of a subsequent investigation at FSU, the AccuVote-OS Optical Scan device, using the most current software revision, has been recertified by the Florida Department of State. The

AccuVote-TSX has not been recertified as of 12/14/07. Florida is currently conducting certification tests on the AccuVote-TSX v4.7.1

8.6 Independent Test Authority Reports (ITA)

Testing of the components used in Alaska for certification against the 2002 VSS (Voting System Standards) was performed by SysTest Labs in Denver, Colorado. SysTest did provide a brief description of the testing procedure used for VSS/VVSG (Voluntary Voting System Guidelines) certification, but were unable to provide any specific testing results to the technical team. Premier has agreed to make a redacted version of the test results available to the technical team for use in this project, but we have not yet received that documentation.

8.7 Summary of Technical Findings

The California TTBR and the University of Connecticut and Florida investigations found many serious vulnerabilities in the same or more current versions of the electronic election systems components used by the State of Alaska. This equipment includes the AccuVote-OS optical scanners, the AccuVote-TSX touch screen devices, and the GEMS server. In addition, each report concluded that additional vulnerabilities would almost certainly have been discovered had there been additional time available to the investigators. The Florida investigators performed a series of subsequent studies (following the initial report) on revised Premier (formerly Diebold) devices after having given the vendor an opportunity to correct the flaws that were found during the initial Florida and California studies. These follow-up investigations on later versions of the software and hardware found that some of the flaws had been fixed, others had been partially fixed, and others remained unchanged.

Many of the recent reports have not addressed the mitigating or exacerbating impact of process and procedures in election voting system implementations. This is an area that the Alaska project will be able to address in Phase 2. Alaska's election system has standard procedures statewide. However, the idea that systems with such serious vulnerabilities might be used to implement elections when protected only by policies and procedures, is akin to a suggesting that a skydiver should take no care while packing their main parachute simply because they also carry a backup parachute.

Even the most carefully designed processes can fail when people are charged with implementing them or when assumptions made and constraints identified while designing the policies change or are flawed from the outset. When such policies do fail it is a good security strategy to have multiple layers of protection in place—the *defense in depth*, which we introduced at the outset of this report. That can help ensure that underlying systems (like the voting system hardware and software) may continue to function at an acceptable risk level even when related components (such as the procedures put in place for the poll workers) have failed.

During the Phase 1 analysis, we identified several areas of the election process for further technical review during Phase 2. In many areas, previous studies have found serious technical vulnerabilities in the same, or more recent, versions of the systems in place in Alaska. The technical areas that require further analysis during phase 2 include:

- The extent to which the vulnerabilities identified in previous studies are mitigated or exacerbated by the policies and procedures in Alaska.
- The communication protocols used within the system, both for the distribution of ballot data to the polling places, and for reporting of results to the Division of Election offices.
- Any potential single points-of-failure in the system, such as the use of a central tabulating server in Juneau for the collection and aggregation of the electronic results.
- The mechanisms used to ensure that election system components are in a known configuration after they have been out of the control of the Division of Elections (e.g., on loan for local elections).
- The methods used to authenticate trusted components of the system.
- The impact of the designation of paper ballots as the official vote in the case of disputes or recounts.
- The cost/benefit of using optional components or more recent versions of the Premier Election Solutions hardware and software.
- The reliability of the AccuVote-OS Optical Scan devices in realistic conditions

In short, the technical components of the system must be looked at in the context in which they are used—the processes, procedures, and people associated with the system.

9 Considerations for the Division of Elections

The Phase 1 evaluation has provided a solid foundation upon which to build in Phase 2. Though each of the technical studies from other states found some unique items, for the most part the reports generally concurred with each other. Given the level of detailed analysis performed by California, Florida, and Connecticut, we are reasonably confident we would not find major surprises were we to conduct our own similar study of the machines Alaska uses.

However, despite the thoroughness of these technical studies, they are not sufficient to show the issues in Alaska's context or identify additional issues that may be unique to our environment.

Armed with this very useful information, we now have the potential to understand how Alaska's processes, procedures, and people can work together to either mitigate or exacerbate election system vulnerabilities.

The Phase 2 scope of work we prepared at the onset of the project included the following items:

Phase 2: Detailed Analysis, Validation and Prioritized Recommendations

- A series of test runs of Alaska's technology with attempts to corrupt the results with existing policies and procedures in place.
- Evaluation of processes for functionality testing, logic and accuracy testing, system security, pre-election and post-election auditing.
- Evaluation and recommendations of data transmittal to GEMS computer to avoid introduction of viruses and long-time delays in election returns.
- An analysis of the process and procedure requirements, to evaluate effectiveness against tampering (technologies, systems and procedures).
- Evaluation of procedures for transportation of election materials and equipment to provide sufficient time for set-up prior to the election while maintaining necessary security of the equipment.
- Evaluate methods to protect system from malicious insiders seeking to affect election outcome
- Suggestions for changes to processes and procedures to increase the security of the elections.
- Evaluation of any security related issues associated with touch-screen voting units

Deliverable: Project Plan to address prioritized list of technology, systems and procedural vulnerabilities phased to meet 2008 election process timeline

Timeframe (estimated): January – End March 2008

Based on the work we have completed for Phase 1, we have validated that several of these items warrant further study, we've identified new items, and found that others many not require further evaluation.

We propose a continuation of the project with a more in-depth Phase 2 evaluation.

10 Proposed Phase 2 Scope of Work

We propose an in-depth evaluation of nine areas in three broad categories that represent a range of potential security risks and public perception.   In some areas, work needs to be sequenced to build a foundation for subsequent work. We also propose continued, close collaboration with the Division of Elections to establish priorities and timelines phased with critical 2008 election process milestones.

10.1 Defense in Depth

10.1.1 Equipment management assessment

- **Inventory management**
  Inventory of software version on each machine and verification that all machines are running same software version. Election officials suggested that we evaluate the cost, requirements, and process to upgrade existing systems if later revisions of system software or firmware become available in time to use in the 2008 election[9] .
- **Storage security and access**
  Document and map where election equipment is stored from one election cycle to the next—including secure storage, loaning to municipalities (State of Alaska, 2007), and repairs. Document security practices in regional offices and hub communities. Assess security in each storage facility. Determine best practices for secure storage and determine whether the same procedures would be feasible in Alaska.
- **Chain of custody, including transportation logistics**
  Document and map the chain of custody for voting equipment from one election cycle to the next (State of Alaska, 2007). Determine when machines are outside of the chain of custody—including transportation and storage at election workers' houses. Document practices when equipment is outside of the chain of custody (State of Alaska 2007), and security checks on election equipment after it is returned. Evaluate risks to tampering or damage/loss when equipment outside chain of custody or in transit.

10.1.2 Personnel policies and procedures assessment

- **Procedural review**
  Evaluate implementation of voting procedures in polling whether procedures are implemented as intended. Identify areas where polling place practices could introduce security risks.
- **Security training**
  This would include training provided by the state and by Diebold for selected officials.
- **Access control**

Identify and trusted personnel in election system and points of access for each. Identify single points of access and superimpose on maps developed in Phase I.

[9] In Alaska, February is the deadline for changes to election systems.

10.1.3 Election processes

- **Absentee and questioned ballots**
  We will apply what we know about the Election Day voting system to Alaska's absentee and questioned ballot system and identify areas of security risk.
- **Paper ballots**
  Identify vulnerabilities of paper ballot system to tampering. Contrast with risks in electronic system. Identify key points in process where tampering could occur are printer, shipper, voter, return to Juneau. Analyze performance/accuracy of optical scanning devices under different scenarios.
- **Personnel Analysis**
  Determine points where redundancy in personnel, procedures and/or joint review processes should be implemented.

10.2 Fortification of Systems

10.2.1 Technical system analysis

- **Contextual System Examination**
  While much of the equipment used in Alaska is similar to that used and studied in other states, there are some unique characteristics about the current and potential future Alaska system that warrant serious investigation. These include the communication protocols used, the integrity and reliability of the hardware and software, and the perceived and real usability features of the systems.
- **System Revision Analysis**
  Evaluation of changes and potential enhancements to the systems that have been implemented by other states and help to determine potential cost/benefit analysis.

10.2.2 Technical processes analysis

- In addition to the physical equipment used by Alaska in its election processes, there are technical processes in place and proposed that should be investigated. These include system configuration options, technical documentation review, and most important, the examination and investigation of election security in the Alaska context which differs significantly from other states' configurations.

10.3 Voter and Election Officials' Confidence in Outcomes

10.3.1 Public perception of election security in Alaska

- **Voter confidence**
  Review information from emails and comments on Phase I report and incorporate public comments into Phase II research design as appropriate. Review of relevant literature to assess

current voter confidence in election security. Identify demographic groups with low levels of confidence. Identify methods to increase voter confidence.

10.3.2 Election results validation

- We will evaluate alternative methods for random sample selection and hand count and determine if they would be more effective at identifying anomalies than the method currently in place.

10.3.3 System and Memory Card Integrity Validation

- Auditing system security. Pre- and post-election auditing. Evaluation of processes for functionality testing, logic and accuracy testing,

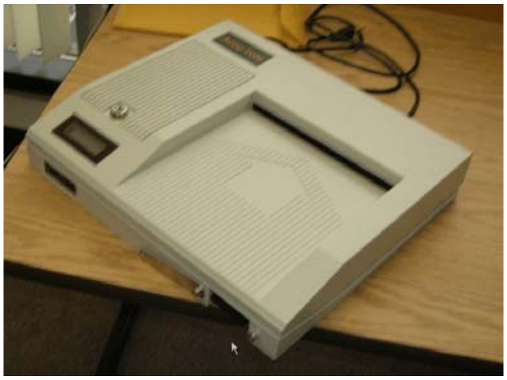
10.3.4 Mechanism for Public Comment

- We propose a weekly review of email contacts from the public. These inputs would be summarized and published on a weekly basis in the form of FAQs or responses to general questions. We would not respond to individual emails. On a limited basis, members of the team could participate in town-hall discussions to answer live questions.

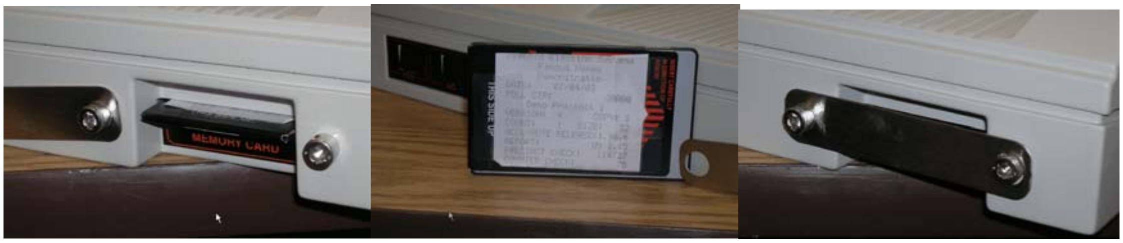
11 Appendix A: Photographs of System Components

11.1 AccuVote-OS Terminal

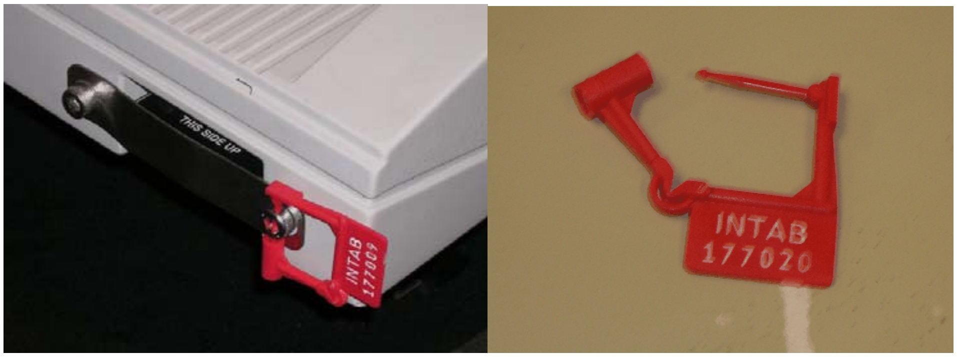
AccuVote-OS (Optical Scan Terminal)



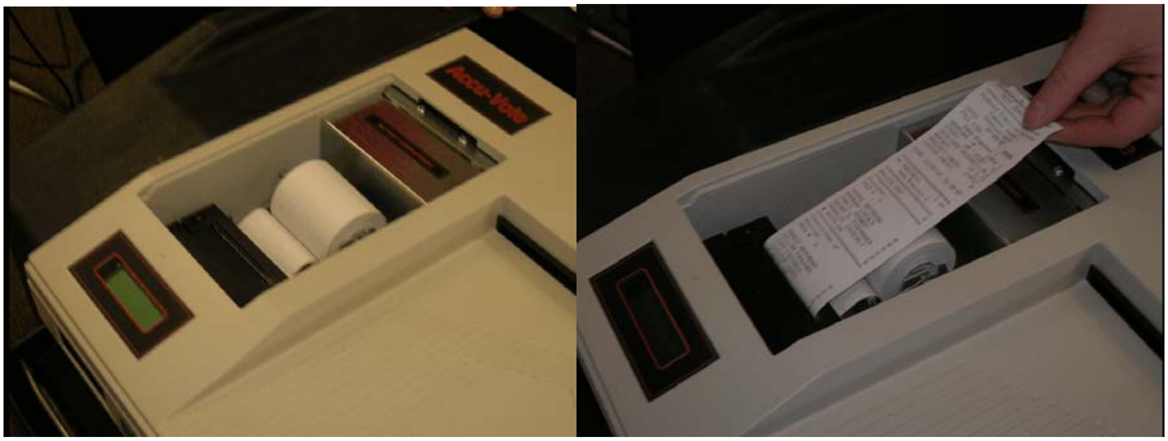
AccuVote-OS memory card port, memory card and panel to secure memory card in terminal.



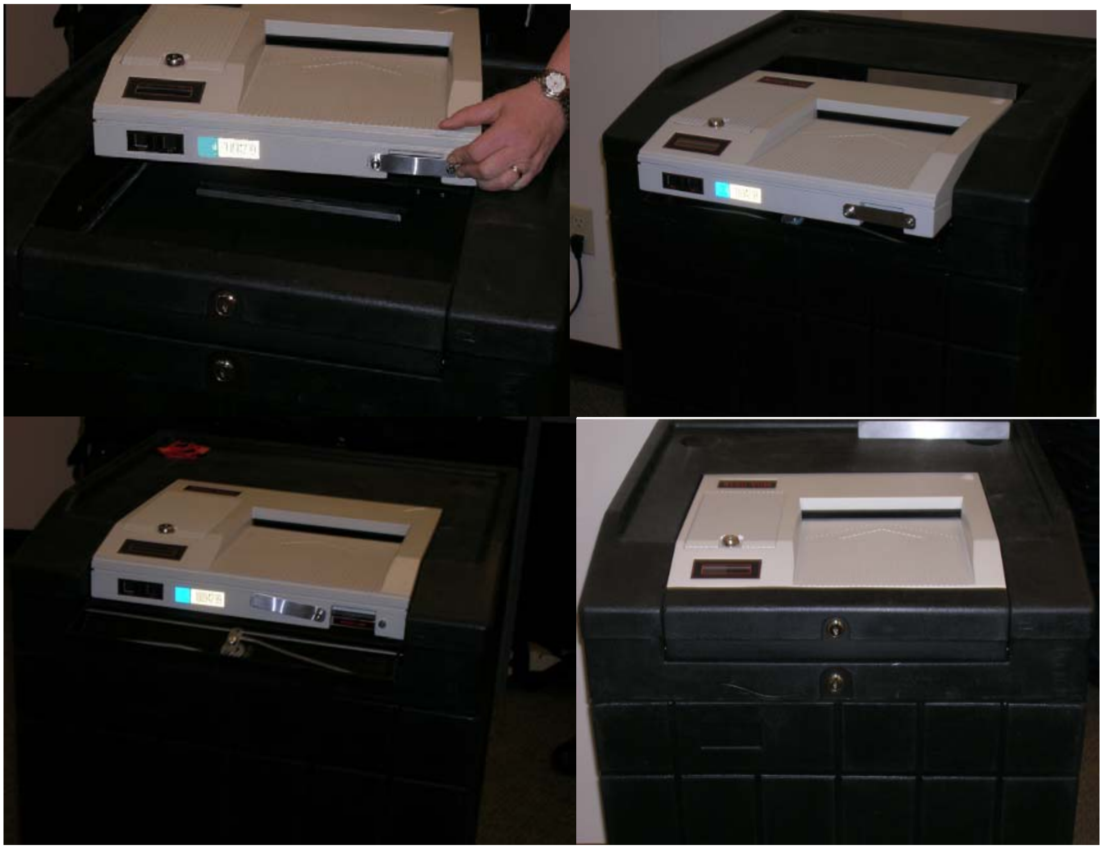
Accuvote-OS Memory Card port secured with tamper evident, numbered tab. Tamper evident tab after removal.



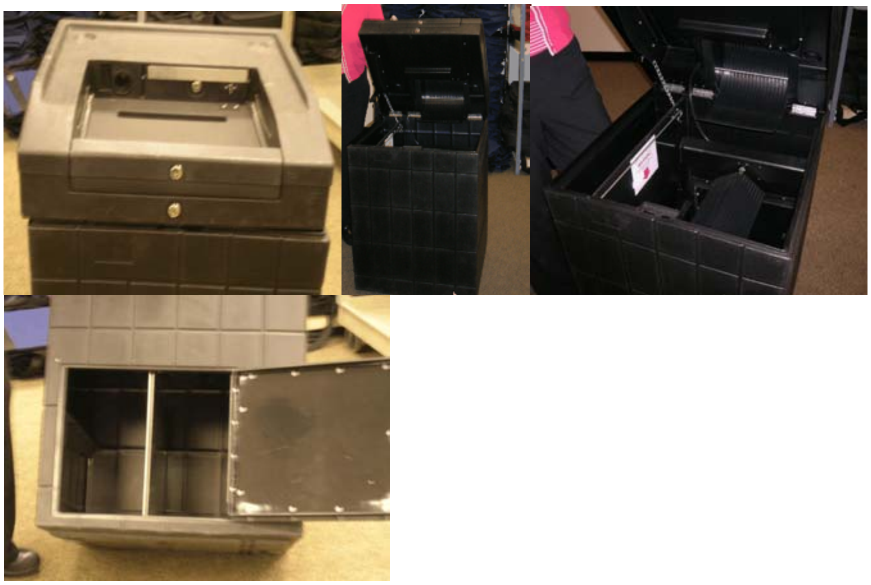
AccuVote-OS Terminal vote recording tape chamber and tape. Secured beneath locked panel during election.



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 cover the secured memory card port and the rear of AccuVote-OS unit (lower right).

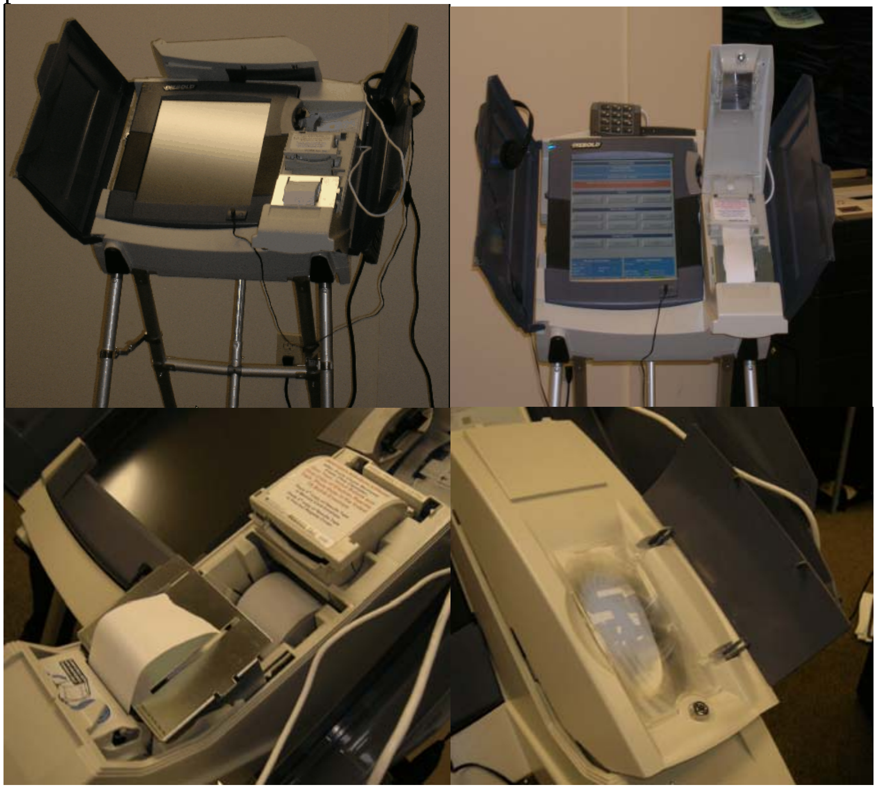


Dual chamber, secure ballot container..

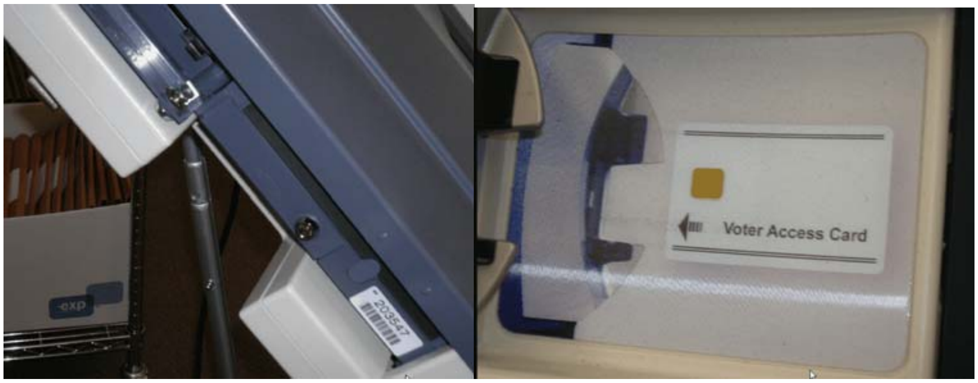


11.2 AccuVote-TXS (Touch Screen Voting Terminal)

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.



11.3 Global Election Management System (GEMS) Server

GEMS Server (Fairbanks and Anchorage)

11.4 Fairbanks and Anchorage Regional Office Equipment Storage

Fairbanks

(At the time of this photo the optical scanning equipment was on loan to the Fairbanks North Star Borough for their municipal election.)

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

12 Glossary

Acronym/Phrase/Name	Definition
AccuVote-OS, AV-OS or OS	Premier Election Solutions optical scanning vote tabulation machine
AccuVote-TSX or AV-TSX or TSX	Premier Election Solutions touch screen voting machine
Chain of Custody	People, processes and locations of equipment and that have authorized custody of election material
CD	Compact Disc
COTS	Commercial-off-the-shelf
Diebold	Previous name for Premier Election Solutions. Name changed in July 2007.
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
Premier Election Solutions	New name for company. Replaces Diebold. Name changed in July 2007.
SAIC	Scientific Applications International Company
SAIT	Security and Assurance in Information Technology Lab (Florida State University)
TTBR	California Top-to-Bottom Review commissioned in Summer 2007
VSS	Voting System Standards
Memory Cards	Removable cards that are formatted with election information and are used in optical scanning and touch screen voting machines to tally results for a given machine.
VVPT	Voter Verifiable Paper Trail
VVSG	Voluntary Voting Systems Guidelines

13 References

Abbott, Robert P., Mark Abrams, Joseph Edmunds, Luke Florer, Elliot Proebstel, Brian Porter, Sujeet Shenoi and Jacob Stauffer. 2007. *Red team report*. July.

Alaska Election Laws and Regulations Annotated. 2006-2007 Edition. LexisNexis

Baker, Rebecca. 2007. Election Supervisor. Alaska division of elections. Nome regional office. November 8. telephone interview.

Bishop, Matt. 2007. *Overview of red team reports*. Accessed 10/15/2007 http://www.sos.ca.gov/elections/elections_vsr.htm

Bradshaw, Sarah Jane. Acting Director, State of Florida Division of Elections. Phone interview, December 11, 2007.

Byrd, Dave, President, Diebold Election Systems, Inc. Letter to Debra Bowen Re: DESI/Premier Response to Red Team Review. August 22, 2007

Calandrino, Joseph A., Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, William P. Zeller. 2007. *Source code review of the Diebold voting system*. Report for the California Secretary of State.

California Association of Clerks and Election Officials, CACEO. 2007. Letter in Response to California Secretary of State draft criteria for a top to bottom review of the state's electronic voting system. Position paper. March 26. Accessed: http://www.sos.ca.gov/elections/voting_systems/ttbr/archive/index.htm May 26

California Secretary of State. 2007a. Frequently asked questions about Secretary of State Debra Bowen's top-to-bottom review of California's voting system. News release. August 15, 2007.

California Secretary of State. 2007b. *Post-election manual tally requirements*. Report. October 25.

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

Celeste, Richard, Dick Thornburgh, and Herbert Lin, eds. 2006.*Asking the right questions about electronic voting*. National Research Council. National Academies Press:

Congressional Research Service. 2003. *Election reform and electronic voting systems (DREs): analysis of security issues*.

Cuyahoga Election Review Panel, Cuyahoga County of Ohio. *Final Report* July 20, 2006

Dictionary of Computing. 1996. Fourth Editon. Oxford: Oxford University Press.

Florida Secretary of State. Undated. *Florida voting system standards*. Florida Division of Elections. Bureau of voting system certification.

Florida Department of State. Undated. Letters.

Gainey, David, Michael Gerke, and Alec Yasinsac. 2007. *Software review and security analysis of the Diebold voting machine software*. Supplemental report for the Florida Department of State. August 10.

Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, Michael Gerke. 2007. *Software review and security analysis of the Diebold voting machine software*. Final Report for the Florida Department of State. July 27.

Growden, Shelly, State of Alaska Division of Elections, *Ballot Counting System Testing and Security-2006*

Growden, Shelly, *State of Alaska Division of Elections, Specifications for Division of Elections Ballot Transportation & Security for the 2006 General Election (November 7, 2006)*

Growden, Shelly. State of Alaska Division of Elections *Accu-Vote Security Enhancements and Features (Provided, October 2007)*

Help America Vote Act of 2002 (HAVA). 2002. Public law 107-252. October 29.

Hoke, Candice and Dave Kettyle. *2007 Documentation assessment of the Diebold voting systems.* July 20. http://www.sos.ca.gov/elections/elections_vsr.htm Accessed 10/15/2007.

Kiayias, A., Michel, L., Russell, A., Shvartsman, A.A. *Accuvote Optical Scan Vulnerabilities and Safe Use*, October 27, 2007. UConn VoTeT Center and Department of Computer Science and Engineering, University of Connecticut

Kiayias, A., Michel, L., Russell, A., Shvartsman, A.A. Electronic Voting Machines: A Summary Comparison of the Optical Scan (OS) and Touch Screen (TS) Voting Terminals, 2007. UConn VoTeT Center and Department of Computer Science and Engineering, University of Connecticut

Kiayias, A., Michel, L., Russell, A., Shvartsman, A.A. *Integrity Vulnerabilities in the Diebold TSC Voting Terminal*, July 16, 2007. UConn VoTeT Center and Department of Computer Science and Engineering, University of Connecticut

Kiayias, A., Michel, L., Russell, A., Shvartsman, A.A. *Preliminary: Optical Scan Memory Card Testing*, November 2, 2007. UConn VoTeT Center and Department of Computer Science and Engineering, University of Connecticut

Kiayias, A., Michel, L., Russell, A., Shvartsman, A.A. *Security Assessment of the Diebold Optical Scan Voting Terminal* , October 30, 2006. UConn VoTeT Center and Department of Computer Science and Engineering, University of Connecticut

Kohno, T., Stubblefield, A., Rubin, A., Wallach, D. (May, 2004). Analysis of an Electronic Voting System. IEEE Symposium on Security and Privacy 2004. IEEE Computer Society Press.

Mara, Leslie. State of Connecticut, Deputy Director of State. Telephone interview, December 11, 2007.

Olovsson, Thomas. 1992. *A structured approach to computer security*. Technical report No. 122. http://www.ce.chalmers.se/~ulfl/webmdemo/wmwork/www/security_122_1.html

Parker, Donn B. 1981. *Computer Security Management*. Reston, VA: Reston Publishing Company Inc.

Posner, Richard A. 2000. *Florida 2000: A legal and statistical analysis of the election deadlock and the ensuing litigation*. Supreme Court Economic Review. Volume 12. University of Chicago Press.

RABA Technologies. 2004. *Trusted agent report: Diebold AccuVote-TS voting system. Report prepared for the Maryland General Assembly,* Department of Legislative Services. January 20. www.raba.com/press/TA_Report_AccuVote.pdf Accessed: 10/15/2007.

Rogers, Kathy. XXXXtitle, Hallmark, Jeff, Iredale, Talbot. Premier Election Solutions. Phone interviews December 11-12, 2007.

Selker, Ted. 2004. *Processes can improve electronic voting: a case study of an election*. Caltech/MIT Voting Technology Project. Working paper. October 2004.

Shamos, Michael Ian. 1993. CFP'93 Electronic voting--evaluating the threat. Report. http://euro.ecom.cmu.edu/people/faculty/mshamos/CFP93.htm Accessed 10/15/2007

Shamos, Michael Ian. 2004. Paper *v. electronic voting records—an assessment*. Accessed 10.15.2007 *http://euro.ecom.cmu.edu/people/faculty/mshamos/paper.htm*

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

State of Maryland. (September 2, 2003). Risk Assessment Report. Diebold AccuVote-TS Voting System and Processes. Retrieved 12/7/2007 from http://www.elections.state.md.us/pdf/risk_assessment_report.pdf

United States Federal Election Commission (FEC). 2002. *Voting systems performance and test standards: an overview*. Vol. 1