

Executive Summary

Alaska Election Security Report, Phase 2

See the back page for a list of contributors

University of Alaska Anchorage

April 2008

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

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

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

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

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

That new system is important. It corrects a number of vulnerabilities in the current system, identified in Phase 1 of this study. But as of April 2008, it had not yet been certified to standards required by the federal Election Assistance Commission. Alaska can't use the new system until it is certified—and when it is certified, it will take a lot of time, money, and people to do the upgrade. It will have to be installed on hundreds of optical-scanning machines, touch-screen devices, election-management servers, and other equipment

scattered throughout Alaska. Taking on such a big, expensive job would not be practical, even if the new system were certified in the next few months. At this point, the Division of Elections is already doing many tasks required before the primary election in August and the presidential election in November. Also, because the state shares voting equipment with local governments, the upgrade will have to be coordinated with them as well.

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

Recommendations for Improving Alaska's Election Security

Change By 2008 Election	Why?	Change After Election	Why?
<ul style="list-style-type: none"> ✔ <i>Verify the accuracy of voting technology before and after the election, by comparing code in voting machines with correct, registered code</i> ✔ <i>Install new software that allows election officials to create a more-secure password authentication system for touch-screen machines</i> ✔ <i>Change passwords on all voting technology throughout the system</i> ✔ <i>Use tamper-evident seals on shipping cases and envelopes</i> ✔ <i>Add election-security material to poll workers' training manual</i> ✔ <i>Increase vigilance about security procedures in absentee polling locations</i> ✔ <i>Purchase state-owned voting machines for use in North Slope Borough, rather than borrowing borough-owned machines</i> 	<p>This series of changes in technology and election procedures will make the existing technology more secure; improve security procedures among election officials and poll workers; and help increase Alaskans' confidence in the integrity of state elections.</p> <p>These measures can all be taken in the short-term, before the August primary and the November 2008 election.</p>	<ul style="list-style-type: none"> ✔ <i>Upgrade voting machines and other technology to new, improved platform</i> ✔ <i>Establish long-term security goals and a method for measuring progress</i> ✔ <i>Improve testing processes to insure all voting technology is functioning properly and recording votes accurately</i> ✔ <i>Develop and implement a standard plan for tracking and changing passwords</i> ✔ <i>Improve system for tracking the number and location of voting machines, through bar-codes or other inventory-control measures</i> ✔ <i>Strengthen storage facilities for voting machines and other system components with dead-bolt locks, alarms, ceiling grids, self-locking doors, and other features to prevent forced entry</i> ✔ <i>Buy more-secure shipping containers for optical-scanners</i> ✔ <i>Recruit and train more poll workers</i> ✔ <i>Consider partnerships with other institutions to do ongoing evaluation and implementation of changes in election-security technology</i> 	<p>Installing the new platform is the single-most important change the state can make, because it will reduce or eliminate risks of vote-tampering identified in the current system. But the platform must first be certified to the Election Assistance Commission's 2002 Voting System Standards, and after that will require an estimated 1,000 man-hours to install on election equipment statewide. Even if it were certified soon, it is not practical now to install the upgrade before the 2008 elections, given the time, expenses, and logistics involved.</p> <p>The other post-election recommendations are either longer-term enhancements of measures recommended for 2008, or additional security measures that there isn't time enough to implement before the 2008 elections.</p>



WHAT IS THE CURRENT SYSTEM?

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

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

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

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

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

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

WHAT MAKES A SYSTEM SECURE?

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

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

VOTE!

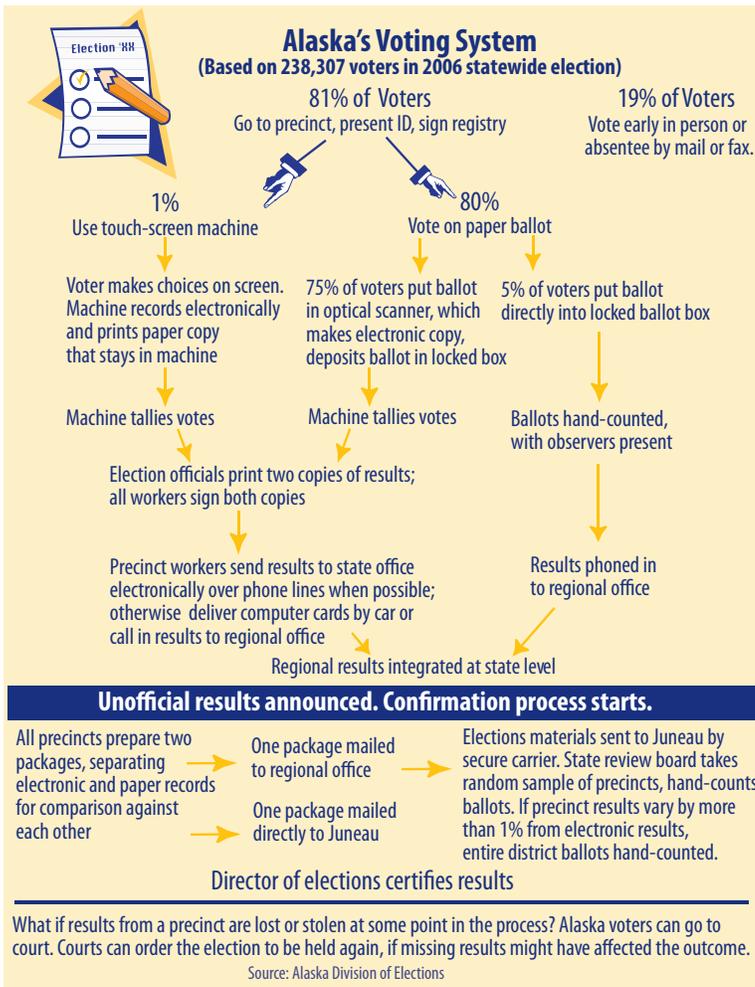
Alaska's Election System



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

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

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



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

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

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

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

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

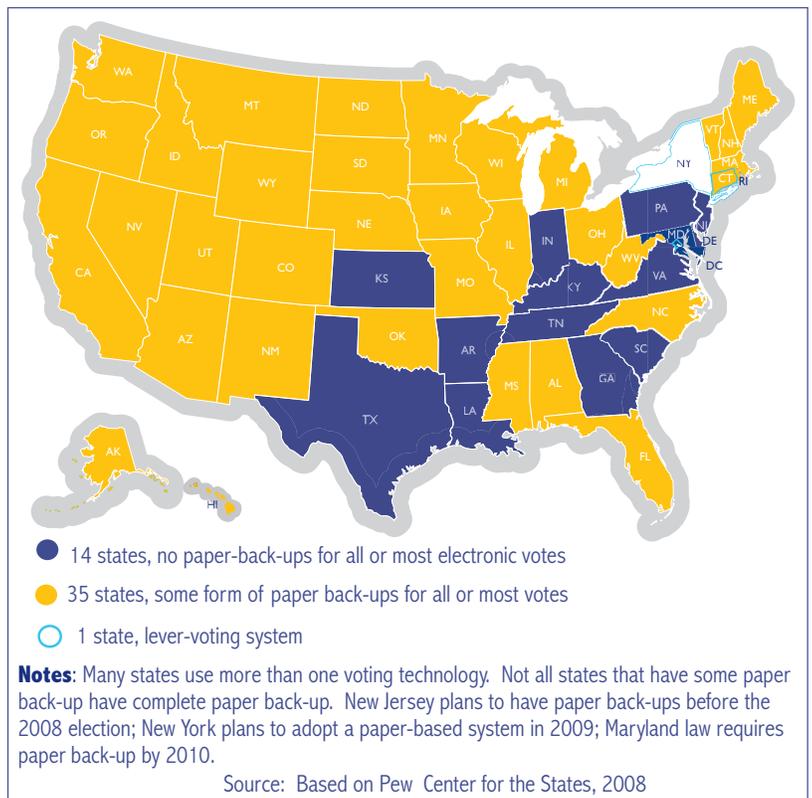
So overall the movement among states is toward systems with paper records—like the system already in place in Alaska.

How Did We Identify Security Issues?

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

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

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



WHAT DO WE RECOMMEND?

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

- **Upgrade to the new, more secure platform after the election.**

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

- **Establish security goals and a method for regularly measuring progress toward those goals.**

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

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

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

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

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

- **Use tamper-evident seals on envelopes and shipping containers.**

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

- **Recruit more poll workers and improve their election-security training.**

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

- **Improve the way voting machines are transported, tracked, and stored.**

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

CONCLUSIONS

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

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

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