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.

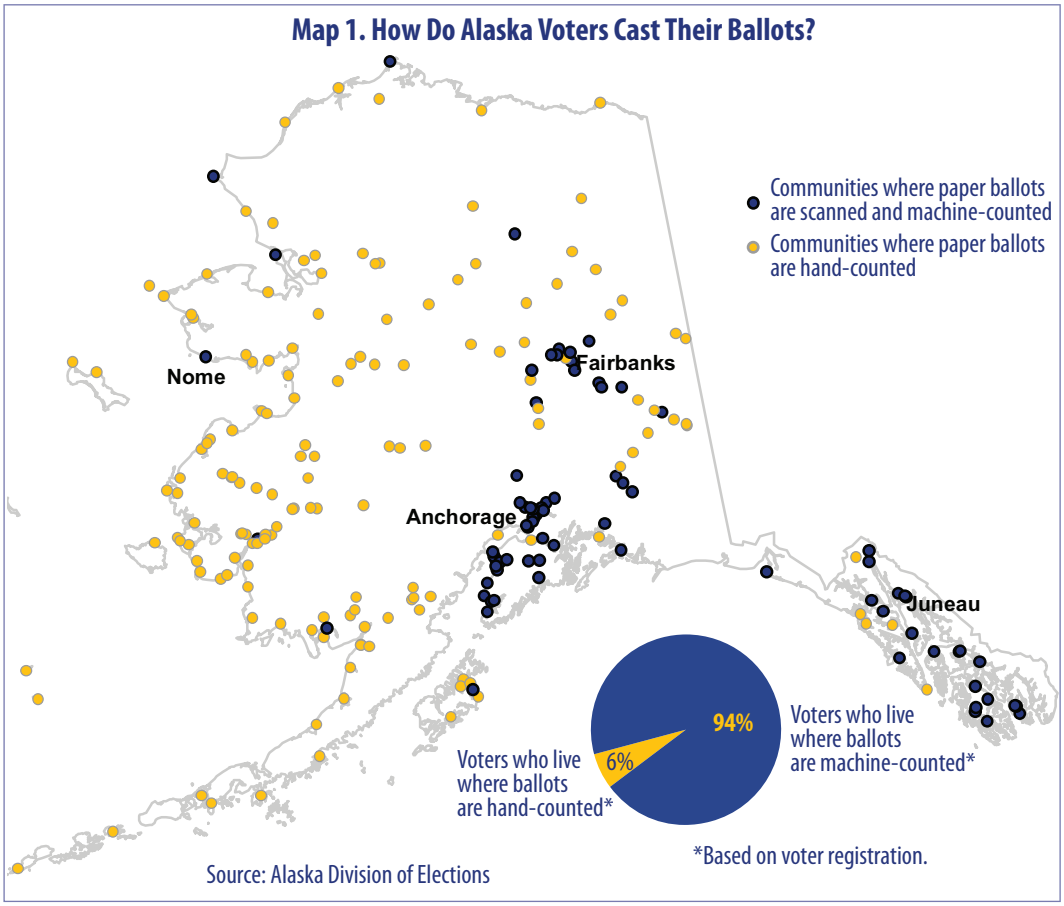
✓ *An open election process that by state law includes observers,* who are able to see both voting and counting procedures.

✓ *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?



*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.

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.

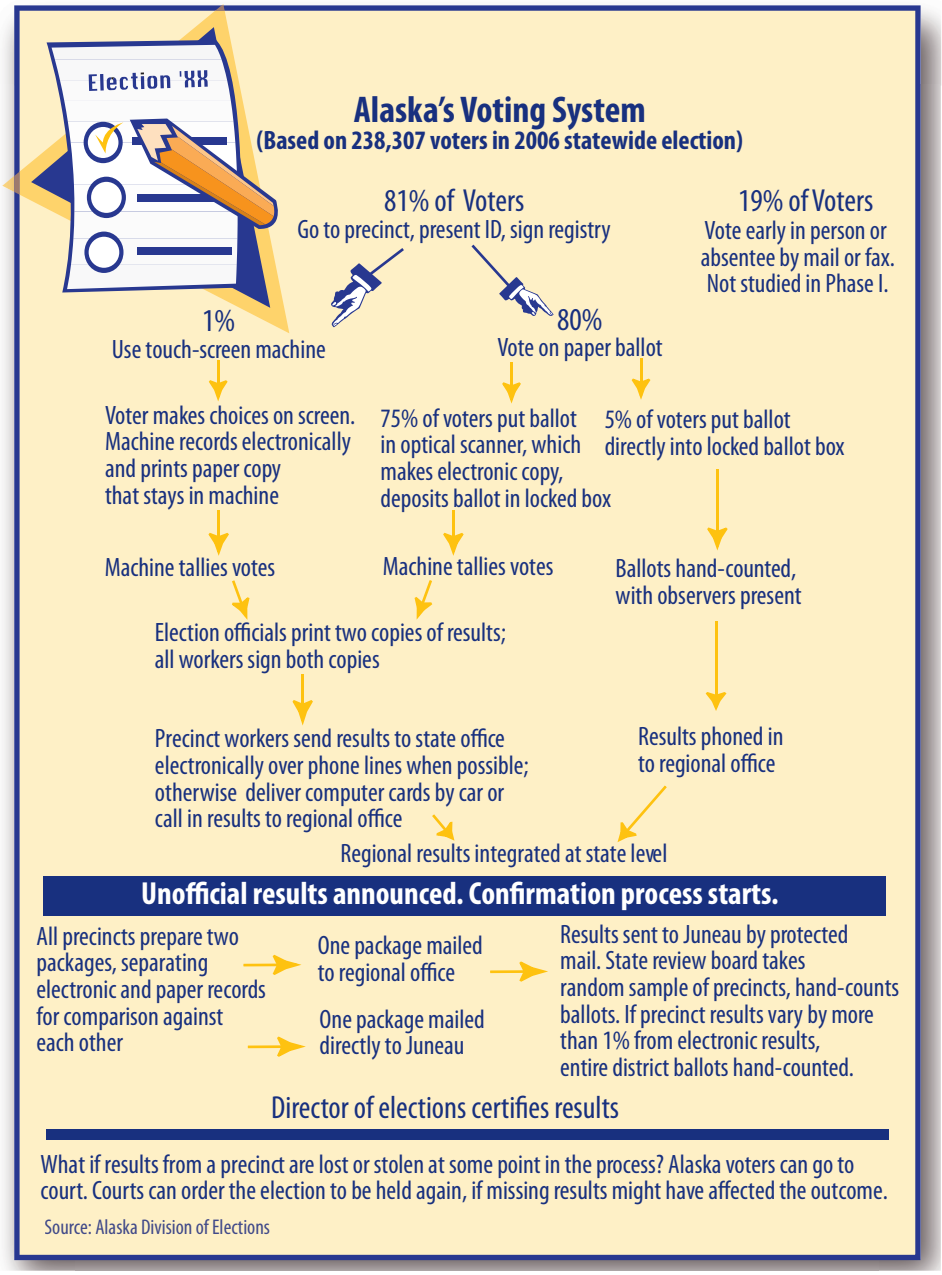
• **Touch-screen machines** are equipped with printers but don't involve paper ballots. Voters touch a screen to make choices. The machine then prints and displays a paper copy, for the voter to verify, but the paper scroll stays in the machines. All 439 Alaska precincts have these devices, as required 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.



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.