

## Executive Summary

# Alaska Election Security Report, Phase 3

University of Alaska Anchorage

April 2013

**A**laska's election system remains among the most secure in the country. But the technology and procedures Alaska uses to ensure that all eligible voters can vote, their votes count, and the results can be accurately reported and certified can use additional improvements. The state's huge size, limited road system, and scattered communities continue to create special challenges for insuring the integrity of the vote.

In this third phase of an ongoing study of Alaska's election security, we recommend some additional ways of strengthening the system. The lieutenant governor and the Division of Elections asked the University of Alaska Anchorage to conduct this additional evaluation, which began in April of 2011, to assess several items from the 2010 General Election Review (April 2011) that were not included in the scope of the earlier Phase 1 and Phase 2 studies completed in 2008. They also wanted to validate the updates to the tabulation equipment that were previously recommended. The goal of this study was to evaluate and recommend improvements prior to the 2012 elections for ballot security, audit post-election processes and hand count verification procedures, ensure that non-US citizens and felons convicted of moral turpitude are not registered or voting, and explore ways to provide real-time voter history information on Election Day.

### What is the Current System?

Election security continues to be a prominent issue nationwide. In Alaska we must continue to evaluate our systems

and procedures and remain vigilant in our efforts to identify and respond quickly to new threats given advances in technology and other security threats. This focus on continuous improvement helps to ensure that the Division of Elections can maintain the public's trust in Alaska's election system. Unlike other election security studies, our studies examine not only voting technology but also policies and procedures that add to the security of the 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.

### Recommendations for Improving Alaska's Election Security

- √ Affix additional tamper-evident seals to the touch screen voting system enclosure
- √ Improve unused and spoiled ballots security at precincts
- √ Strengthen the details of handling voted ballots in Juneau before hand-count verification
- √ Continue efforts to strengthen integration of Alaska State Department of Corrections, and U.S. DHS (Immigration)
- √ Utilize a new comprehensive Election Auditability Checklist
- √ Implement a consistent and effective procedure to provide public record voter history information to interested parties on Election Day
- √ Should not undertake implementation of a stand-alone, real-time voter history solution without further evaluation and within the context of a more comprehensive, long-range electronic voting technology plan including a near term statewide voter registration system upgrade
- √ Develop a mid-to-long range plan for the State of Alaska's election system



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 438 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 305 of Alaska's 438 precincts, almost all voters in Alaska 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 cannot 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.



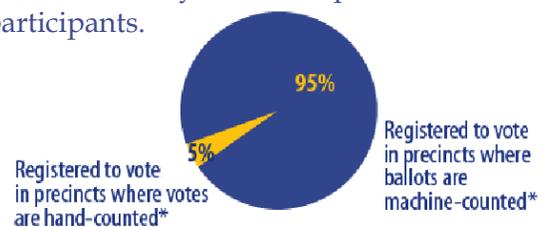
### Alaska's Election System



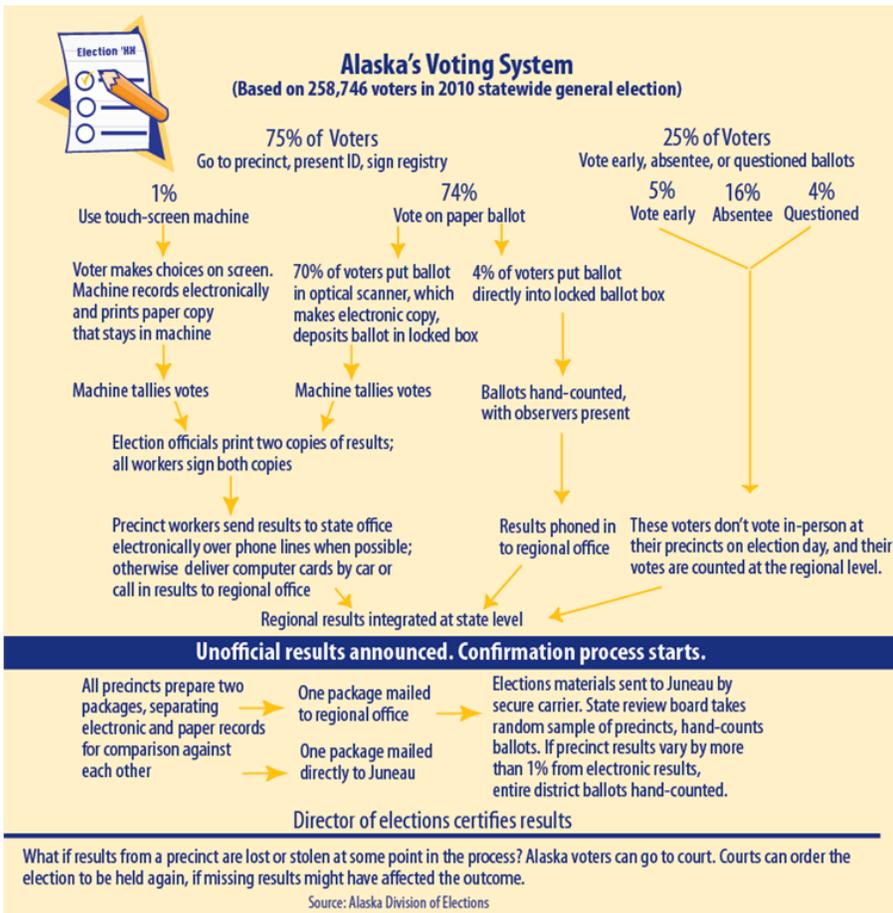
So sending ballots and election equipment to and from communities around the state, as well as storing equipment in small communities with limited facilities, is very expensive and poses many logistical challenges. Also consistent application of processes across all 438 geographically distributed precincts is challenging.

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 attempts to corrupt election outcomes, because several undetected steps would have to be taken 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. These systems and procedures include the equipment and processes used for voter registration, voter eligibility, ballot security, vote tabulation and verification, and procedures used before, during and after elections by officials, poll workers and public participants.



\*Based on 2010 voter registration of 494,876



## How Did We Assess Phase 3 Security Issues?

- We re-validated updates made to the equipment based on the 2008 report recommendations to ensure that the changes made addressed the identified security risks and to identify any new threats.
- We studied ballot security from election planning to final certification.
- We assessed the procedures used to verify voter eligibility to ensure that non-US citizens or felons convicted of moral turpitude were not voting.
- We evaluated post-election processes and hand-count verification procedures.

We found that Alaska continues to be well-positioned, compared with many other states. But we also want to emphasize that every state faces different security and procedural challenges. There is no single solution right for every

state. There is also no perfect system so there are always opportunities for improvement and fine tuning.

We found that all of the updates to the equipment recommended in the 2008 report were completed.

There were further recommendations for additional tamper-evident seals for the touch screen equipment.

We found that there were opportunities to further secure and segregate un-voted and spoiled ballots from completed ballots and to improve their handling and documentation. We found that the division has procedures in place to validate voter eligibility and works with other federal and state agencies to routinely update the voter registration data base with the most currently available information. The processes to collect this information and update the voter registration are not automated. It requires on-going diligence by division personnel to routinely seek out and update this information coming from other agencies.

The division has post-election and hand-count verification procedures that ensure accuracy and transparency. An election process audit checklist was prepared and proposed for use by the division.

As reported in 2008, two aspects of Alaska's system continue to help its election security relative to that in other states: centralization and paper ballot back-ups for virtually all votes.

- **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 of 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 in the system for both voters and election officials. 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 choose different equipment and 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, equipped with an internal paper reel that records votes.

### Real-time Voter History

In addition to the above security items, we evaluated solutions that could provide publicly available, real-time voter history (RTVH) online on Election Day. We assessed commercially available electronic poll book-based solutions along with some possible custom approaches and provided a cost/benefit analysis of those alternatives. We also provided information about how other states make this information available.

### What Do We Recommend?

The table on the front page summarizes our main recommendations, some of which the Division of Elections put into effect before the August primary and the November general election. Here we explain more about some of the most important recommendations, which are discussed in detail in the full Phase 3 report.

- **Affix additional tamper evident seals** to the AV-TSX (Touch Screen) voting system enclosure.
- **Improve unused and spoiled ballot security** at the precincts.
- **Strengthen handling of voted ballots after receipt in Juneau** and prior to hand-count verification.
- **Continue efforts to strengthen integration of Alaska State Department of Corrections, U.S. Department of Homeland Security (Immigration), and other databases with the Voter Registration database.**
- **Utilize a comprehensive Election Auditability Checklist** before, during and after each election.

- **Ensure implementation of consistent and effective procedures to provide public record voter history information** to interested parties on Election Day.
- **Should not undertake implementation of a stand-alone, Real-time Voter History (RTVH) solution** without further evaluation and within the context of a more comprehensive, long-range electronic voting technology plan including a near term statewide voter registration system upgrade.
- **Develop a mid-to-long range strategic plan for Alaska’s Election System** (given expectations that some equipment used in Alaska will soon become obsolete), that includes the evaluation, adoption, and implementation of new technologies (including tabulation systems, databases, real-time voter history solutions, voter registration systems, electronic poll books, etc.) to support the changing needs of voters and election officials in Alaska and that address the associated and necessary evolution of procedures and workforce training to ensure a continuation of secure and participative elections.

### 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 have adopted 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 3 of the *Alaska Election Security Report*, prepared for Lieutenant Governor Mead Treadwell and the Alaska Division of Elections.

Contributors are UAA faculty, staff and researchers: LuAnn Piccard, Mark Ayers, David B. Hoffman, Roger Hull, Michelle Webb, Stephanie Martin, Mary Killorin and Patricia Deroche.