Expert and Peer Security Reviews of Elections Ballot Tabulation Upgrade Business Case

A Report to the Metropolitan King County Council

From
Douglas W. Jones and Eric Lazarus
Lazarus Technology Mentoring, Inc.

July 2007

Table of Contents

Scope of Work

In 2006, King County adopted an ordinance authorizing vote-by-mail elections to begin in 2007 or 2008, after certain conditions had been met, including the ability of voters to track their ballots. In separate legislation, the Council appropriated funds for the purchase of elections equipment and software with the condition that funds for ballot tabulation and ballot tracking and signature verification be expended or encumbered after the Council reviews their business cases.

In March 2007, the Executive transmitted to Council a Ballot Tabulation Upgrade Business Case. And in May 2007, the Executive transmitted to Council a Ballot Tracking and Accountability Business Case. In summary, to facilitate the transition to all-mail voting, the Executive has proposed in these two business cases to purchase equipment and software for the following three election functions:

1. High-speed ballot tabulation, to handle the larger number of paper ballots that will need to be counted centrally with all-mail voting, rather than counted in local polling places. (Ballot Tabulation Upgrade Business Case.)

2. Mail ballot tracking, so that voters and election administrators will be able to track their ballots to confirm that they were received (and possibly, that they were counted). Outgoing and incoming ballot tracking would also allow the county to collect performance measures on late delivery rates and delivery failure rates. (Ballot Tracking and Accountability Business Case.)

3. Signature verification, to expedite and streamline the process by which signatures on ballot envelopes are compared with signatures on file to verify that each incoming ballot was submitted by a qualified voter. (Ballot Tracking and Accountability Business Case.)

In April 2007, because election security is a high priority, the Council voted to have citizen, expert and peer security reviews of these two business cases. The scope of work for the citizen review was to: (1) review the two business cases for purchase of new election equipment and software from a security perspective; and (2) solicit input from citizens on election security concerns. The citizen review was conducted by the Citizens' Election Oversight Committee (CEOC) and presented to the Committee of the Whole on July 16, 2007.

The scope of work for the expert and peer reviews was to review the business cases to determine whether the business cases conform to applicable best practices regarding election security and the recommendations contained in a Brennan Center for Justice report entitled "The Machinery of Democracy: Protecting Elections in an Electronic World."

The Brennan Center for Justice is a non-partisan public policy and law institute that focuses on issues of democracy and justice, such as voting rights. In 2005, the Brennan Center convened a task force of experts to conduct the nation's first systematic analysis of security vulnerabilities in the three most commonly purchased electronic voting systems. The task force's report is entitled "The Machinery of Democracy: Protecting

Elections in an Electronic World" and was peer reviewed by the National Institute of Standards and Technology.

This report presents the expert and peer security reviews of the Executive's Ballot Tabulation Upgrade Business Case. A separate report presents the expert and peer security reviews of the Ballot Tracking and Accountability Business Case. The reviews shall:

- Assess the analysis and recommendations contained in the business cases and compare the recommendations with any alternative courses of action that could be considered;

- Identify the respects, if any, in which the business cases deviate from applicable best practices regarding election security and the recommendations contained in the report entitled "The Machinery of Democracy: Protecting Elections in an Electronic World;" and

- Recommend changes to the business cases, including, if appropriate, recommendation of different equipment and software for purchase, that would bring King County Elections into compliance with applicable best practices and the recommendations contained in the report entitled "The Machinery of Democracy: Protecting Elections in an Electronic World."

The Council selected Lazarus Technology Mentoring, Inc. an independent elections security firm, to complete this scope of work. *(Qualifications of the team of Douglas W. Jones and Eric Lazarus may be found in Appendix One of this report.)*

Expert Security Review

Consultant Recommendations

1. We present several best practices for the county to consider in improving elections processes, such as: Improving security threat education and prioritizing business process improvements before new technology acquisition.
(See Best Practices for Secure Elections Process Improvements Section on page 5 .)

2. We also recommend that the county consider undertaking a best practice process for the acquisition of elections technology.
(See Best Practices for Acquisition of Secure Elections Technology on page 10.)

3. We believe that security be substantially upgraded in important respects without acquiring new elections technology. For example, we strongly recommend that the county advocate for a change of state law that would allow or better, require, counties to perform automatic audits of vote-by-mail ballots and then implement them in King County. Without such a change in the law and instituting audits, the level of election security achieved in King County will be the lowest level measurable according to the methodology of the Brennan Center for Justice report entitled "The Machinery of Democracy: Protecting Elections in an Electronic World."

4. We believe that the safest and most practical option involves delaying acquisition of new technology until after the 2008 presidential election when better systems and more data about the systems will be available. This alternative would reduce risk of election problems since familiar technology would be used rather than new and untried technology.

5. We believe that it is best practice to first upgrade security procedures and the knowledge and skills of election staff with regard to security and, only after that, begin Request For Proposal (RFP) processes. Staff will then be in a position to automate improved processes and will be better able to evaluate the security claims of vendors. Such process and knowledge upgrades are relevant, in our view, for King County.

6. If cost containment and improved security are goals, we recommend the county employ innovative approaches to technology support for elections, including open-source development of election technology designed for secure operations. We believe that if open source options compete on a level playing field with commercial offerings in all future elections technology request for proposals (RFPs) it will lead to better electrons at much reduced cost. We believe that arrangements can generally be made under which the county will take on little or no risk and only pay for the open-source technology after it is has been shown to be appropriate to the County's needs.

7. The number of major changes envisioned for the 2008 presidential election (e.g. acquisition and implementation of a new and untried central ballot scanning technology, moving to a new elections facility and implementing vote-by-mail) is a challenge that does not conform to best-practice norms. We recommend that the county consider scaling back the number of changes for the 2008 election and, specifically, consider not acquiring new ballot tabulation equipment so close to the 2008 presidential election.

Best Practices for Secure Election Processes

Security relies on trained professionals and secure processes, as much as, if not more, than it relies on technology. Therefore, we examine best practices in election processes and then examine best practices in technology acquisition.

Best Practices for Secure Elections Process Improvements

We have identified the following best practices the county could consider to improve voting system security and education:

1. Prioritize staff security, and threat awareness training and key business process improvements *ahead* of the acquisition of new technology.

Prioritizing staff security, threat awareness training and key business process improvements for security ahead of the acquisition of new technology is best practice for several reasons:

- The knowledge that staff will acquire in improving security is likely to enable them to be wiser at both developing the request for proposal (RFP) process and at assessing the responses.

- The increased commitment to security that will naturally emanate from the knowledge, planning and, most importantly, acting on the resulting business process plans with increased security awareness, will raise staff standards and elevate expectations – both for vendor products and services.

- An election team in the process of negotiating contracts and working out the unavoidable kinks in new technology and/or learning to use new equipment will have to divide resources and so will be generally less able to implement enhanced security.

- Technology purchased now, prior to staff security training, that supports the less secure current election processes might not fit well with improved processes designed to be more secure. So the county might need to replace technology that was recently acquired as a result of the security analysis. This can be costly.

- Focusing on a security upgrade process could provide an opportunity for the county to set clear priorities, which then can be used to assess the relative merits of various offerings. For example: Is King County willing to reduce accuracy in order to increase the speed of election returns?

We recommend that the county implement this best practice by conducting a more extensive security review before purchasing new elections technology. The review could evaluate the current elections security process and set clear priorities for improved procedures.

2. Educate election officials on potential security threats.

A critical best practice is education of elected officials on election security. In order for systems to be made secure, elected officials who are making policies for the election processes and those managing and operating the voting systems could be focused on security. Best practice is to understand what attacks are possible, how attacks can occur and what defenses are effective against those attacks. Best practice is also to understand vulnerabilities in terms of the potential they create for future attacks and to avoid relying on the absence of past attacks.

The County could consider additional training for elected officials and elections management on security, possibly by outside experts in the field of security to ensure "fresh eyes" are looking at the county's situation.

3. Process ballots in batches containing only one precinct or card style

A best practice in mail ballot voting is processing ballots in batches containing one precinct or ballot style in order to avoid the inadvertent revelation of any single voter's voting choices. Batches should be of a size that can be processed through each individual station of the ballot path in one work shift and with the same observers who are able to watch an entire batch processed. Security is compromised if a batch is spread over two different sets of observers, as the reconciliation at the end of the batch is just as important and directly related to the work done in processing the batch. In addition, if an error in a batch is found, it is easier to reprocess a smaller batch to discover the error. Batch sizes should not be so small that privacy is compromised. For example, if a voter was the only representative of their precinct included in a batch, then the batch totals will disclose that voter's votes for every race on the ballot if the batch totals are broken down by precinct.

In order achieve ballot privacy, a key security goal, we recommend that the county consider processing ballots in batches that are sorted at the precinct or ballot style level. This would enable individual voter choices to be kept confidential. As the number of ballot styles included in a batch grows, the chance of violating the voter's right to a secret ballot grows because of the possibility that only one ballot of some style will be included in a batch.

4. Seek a change in state law to allow automatic routine audits for mail ballots

Statistical audits (what the Brennan Center Report termed Automatic Routine Audits) are a security and error-detection measure used in many places. For example, the State of California law requires every county to audit by hand at least one percent of the ballots.

Best practice for an audit of this type involves the following steps:

- Ensure good chain-of-custody of paper and electronic records. This is essential, because if an attacker can hide the evidence by providing fake paper, then the audit will be meaningless.

- Allow observers and auditors to see and have the numbers being audited and evidence that those numbers make sense in context, i.e., that they add up to the total published election results.

- Select the items being audited. The goal is that an attacker will not be able to determine which batches of ballots will be audited, otherwise an attacker can subvert the audit. Also, since the audit can detect errors, a random sample is useful. Best practice is to randomly select, after the election results are supplied to observers, the items to be audited. Another best practice is to make the process of how ballots were randomly selected transparent. This will enable elections observers the ability to observe if the random selection was indeed random.

- Auditors count the paper records and report them to observers and election officials publicly.

- The observers certify that the results from the auditors match the committed numbers they were supplied in step two.

King County currently does not perform a statistically valid audit on vote-by-mail ballots. It appears that state law, under some interpretations limits the county's ability to do so. The county does an audit for the Accessible Voting Units, but does not follow the best practices outlined above.

We recommend that the county advocate for a change in state law or obtain a Secretary of State administrative rule dispensation to perform automatic routine audits on vote-by-mail ballots. County procedures and training would be modified to reflect these audit procedures which would improve protection against fraud and error. These audits provide a general and powerful way to verify that the elections machines are capturing and counting votes correctly. Relevant resources include a report from the Brennan Center for Justice and University of California at Berkeley that provides effective audit procedures.

5. Test all systems and sites against intrusions

Intrusions are tests of a system that are designed to learn about the security of a system. For example, tests are performed to see if system security can be defeated, if procedures are being followed, and to discover new types of attacks that could be guarded against.

In banking and other industries where higher levels of security consciousness are common, qualified and trusted individuals or teams are hired to try to break into the physical location and/or computer system. This is a best practice for elections as well. Such exercises have the following effects:

- Deterrent Effect: If staff know the repercussions of violating security protocols, they were to allow someone, perhaps a painter (really a security expert hired to test the security) into a secure area, it is safe to assume that they will be more motivated to follow procedure and "think security." The same is true for vendors.

If they know that their software is going to be tested, they will be more motivated to do a more complete security test on their system.

- Motivating Effect: When vulnerabilities are found, they can often be addressed better after the problem has been dramatized by an exercise because a demonstration provides urgency and motivation that a white paper often does not.

- Discovery Effect: Intrusion experts are often very creative. Their work can augment counties' threat models that can then drive the implementation of better security policies. This makes the entire system safer.

No such approach is being utilized by King County, nor does one currently appear to be planned. We recommend that the county conduct such exercises on a regular basis.

6. Observe and report on ballots by batch

We believe it is important that election observers at the tabulation center receive reports on each batch of ballots as it moves though the workflow. In particular, we recommend that observers be provided with official written records during the course of each day reflecting the status of each batch and when each batch gets to each stage of processing, how many ballots arrived in each batch, and what the outcome was of that process, e.g., how many ballots in that batch had their signatures verified, who did the verification, who entered the information into the tracking database, what happened to the ballots that did not verify, etc. We call this practice "batch-level transparency" and consider it a key security and accuracy measure.

In King County observers can currently see from a bit of a distance that certain processes are taking place, but observers are not currently permitted to monitor the progress of batches. The county could arrange for a persistent record to be created and displayed for all observers to see and analyze. Observers are there to witness to the election and we recommend that every effort be made to enable them to testify to the quality of the work being done and the accuracy of the election result.

7. Evaluate ballot design

Ballot designs impact voting. A best practice is to conduct tests, employing real voters, of all ballot forms to ensure that they are not confusing to the voter. Past experience shows that large and highly variable error rates by voters are inevitable unless testing is performed and corrections made.

We recommend that the county perform tests before each election to ensure that confusing ballots do not disenfranchise voters. This is particularly important where all-mail voting is used, since voters have no chance to correct errors that they might have corrected themselves when using precinct-count mark-sense scanners.

8. Negotiate enhanced vendor support for security

A best practice is to contract for adequate vendor support for security. King County may choose to consider negotiating with it current vendor to enhance security support. For example, enhanced vendor support could be added to require the vendor to fix critical security problems in a timely manner after notification to submit the fix for federal and state certification. Ideally, in our view, these negotiations should be performed by purchasing professionals with a security background (or consulting support) rather than by the election officials who must maintain close relationships with vendors. It is best practice also to perform those negotiations before a final decision has been made with regard to what vendor will be selected because the county naturally remains in a stronger negotiating position before the Council commits to a final decision.

9. Prepare and employ a handbook for Election Observers

A best practice is to document the approaches used by the most effective election observers.

The county could consider defining the responsibilities of observers and preparing an Election Observer handbook. The handbook could include checklists of things to look out for and forms to fill in to document that activities have been observed in a meaningful way. The use of a handbook could be used to evaluate the performance of observers. For each of the workflow steps and business processes, there could be item the observer can observe. The handbook could also familiarize the observer with various attacks and sources of error and how they could be detectable by an observer.

Some relevant starting points would be the Code of Conduct for International Election Observers, United Nations, 2005, and the Election Observation Handbook, OSCE ODIHR, 2007. These are generic but very useful.

Best Practices for Acquisition of Secure Elections Technology

Following is the best practice process for security-sensitive technology acquisition decisions, and we recommend that the county consider undertaking this process:

1. Examine the options

Develop best practices and then examine technology that supports those practices. It is not a technology acquisition best practice to select the technology first and then attempt to adjust the business process to fit the technology.

2. Establish critical success measures

Determine the measurements of the project's success. For example, "Increase processing of ballots by x days/hours/minutes."; "Number of challenged ballots is reduced by x."; "Reduce cost of election by $x."

3. Define the problem

Before attempting to design or select technology, it is important to understand the problem that is being solved. For example, what are the basic operations in the process you intend to automate, how do these operations relate to each other in your solution to the problem, and what does it mean to do each process, in terms of the priorities and assumptions that have been established?

4. Staff the acquisition team

The process begins by creating a team with the knowledge and skills to perform the acquisition which may include more than existing county staff. The team may well combine full-time staff and outside consultants in cases where special expertise and experience are required. We recommend that the team have broad experience with alternative solutions to the problem domain, including experience with multiple vendors, to reduce the risk that the acquisition process limits vendors. We recommend that the team have the authority to commit the organization to policies governing the use of the acquired technology and a willingness to commit to procedures. Election technology without procedures cannot be evaluated so both effective public comment as well as useful legislative oversight are likely to be diminished.

5. Understand and document the core technology

Members of the acquisition team could get training and/or do reading to ensure that they all understand the basics of how the relevant technology works. They do not all need to be computer specialists, but if the knowledge base is insufficient, potential issues may not be identified.

6. Understand and document the threats

Key decision makers and the acquisition team need a clear understanding of security threats so that they can evaluate vendor proposals.

7. Understand and document the countermeasures to threats

Those participating in the acquisition process need to understand the logic of various countermeasures to threats incorporated in the vendor proposals. Each countermeasure could be examined in terms of what threat or threats are addressed and in terms of how the countermeasure deters an attack or decreases the likelihood of a failure.

8. Set and publish priorities and assumptions

Determine the criteria to be used in evaluating threats to the system and clearly document the assumptions underlying these criteria. This needs to be done early in the process, so that policy makers have an opportunity to review and approve the policies and assumptions. Criteria may include accuracy, cost, reliability and transparency. The relative importance of these criteria could be determined early and communicated to the public and vendors.

9. Develop a Request for Proposal (RFP)

Create an RFP document that will motivate those who have or can construct solutions. The RFP could clearly document the proposed evaluation process, including any preliminary evaluations that will be used to limit the number of fully developed proposals that need to be evaluated, and the extent to which policy makers and the public will be involved in the acquisition process. The RFP could be written to require those proposing to expose, as much as possible, all relevant criteria for selection including cost of acquisition, cost of operation, and relevant contract terms.

10. Advertise the RFP broadly

Invite broad participation from all vendors in order to ensure that the maximize number of possible vendor solutions are considered.

11. Evaluate the responses

To avoid the expense of a complete evaluation of all proposals the RFP and evaluation process may be staged. RFPs can be subjected to preliminary evaluations prior to a second round in which a reduced number of vendors are asked to develop complete RFPs.

Responses should be fairly considered in the context of the ideal system architecture, threat models and evaluation criteria. During this process, negotiate desirable contract terms, including security-relevant draft clauses, before the decision-making process is complete. For government acquisition of critical technology, inviting public comment prior to the completion of each round of the evaluation process might be appropriate. Whether in a public or private context, policy makers may choose to observe the process.

12. Make selection

Enable policy makers to make a fully informed decision based on meaningful insight into security and all other relevant issues. This involves developing decision-making materials including how each possible option, including not acquiring new technology meets the criteria outlined and why.

13. Educate operations staff

Before the acquisition process has been completed, it is important to communicate with the staff that will operate the system. They could understand the logic of the acquisition, and the security practices that were assumed in the evaluation. This education will assist the system operators to ensure the system conforms to the acquisition team's assumptions.

14. Implement

Develop a detailed plan for implementing the system within a reasonable timeframe, depending upon anticipated roll-out date, agreed upon by both the county and vendor before signing the contract with the vendor. Then monitor the plan daily to ensure that the schedule and costs are within the original plan. Make adjustments as necessary and incorporate into the plan.

15. Test and audit

Once a system is implemented, it is important to monitor its use and evaluate the system and processes against the success measures established in step two. The policies and procedures that surround systems frequently evolve with time and, therefore system assumptions may need to be reevaluated. If changes are made to system assumptions, they should be documented.

Analysis of Executive Recommendation

The Executive recommends upgrading the existing ballot count tabulation system. The Executive's rationale for this upgrade is that countywide vote-by-mail election cannot be accomplished using the existing system for three reasons:

1. A database size limit;
2. Optical scan machines are breaking down and becoming unreliable; and
3. Pre-scanning of ballots is necessarily in order to have timely election results.

Because we believe that the three problems can be addressed securely and with less risk of system failure without the move to new technology in 2008 for the reasons described below, we do not recommend the purchase and implementation of new technology prior to the 2008 transition to vote by mail.

Database Size Limit

King County experiences the possibility of hitting a two-gigabyte size limit on the ballot tabulation database. This is a well-known issue that the county successfully addressed in the 2000 and 2004 presidential elections. In addition to the Executive's recommendation, King County has several options for addressing this limitation including:

1. King County could sort ballots into batches by precinct before tabulation. With fewer precincts in each batch, the database size will grow at a far slower rate.

2. King County could save the database more frequently, as each time it is saved, data is compressed, and this prevents to 2 Gb size ceiling from being reached.

3. King County could split the ballot tabulation database in approximately two even halves, by legislative districts. With proper determination of which districts to place in which half, whole legislative districts, city and special purpose districts could be placed in one database.

   The aggregation of summary total for the countywide races, such as state and federal races would be accomplished in exactly the same manner as the Secretary of State aggregates statewide races to certify statewide elections. For example, voters residing in Seattle and the northwest part of the county could be placed in one database and voters residing elsewhere in the county could be placed in another database.

   This recommendation would be even more effective for the county if coupled with two arrays of 30 scanners supporting each database, as described in the next section.

Optical Scan Machines

Currently there are 40 optical scan machines that are used for central counting, and the Executive has stated that these machines are breaking and are unreliable. However, the county owns more than 500 optical scan machines that have been used relatively lightly in polling places. If the county goes vote-by-mail for 2008, these additional optical scan machines could be made available to replace the current broken and unreliable machines should they become broken and/or unreliable.

- The county could also use two arrays of optical scan devices, with 30 devices per group. Elections warehouse staff have confirmed that 60 functional, maintained feeders exist in the elections warehouse for use and there are sufficient optical scan devices for a two–array option. Sixty units would be roughly 3.75 times more scanners than were used successfully in 2000, another presidential high-volume election.

Pre-scanning of Ballots

The existing system is not certified by the state to "pre-process" ballots. Pre-processing ballots refers to collecting the vote data prior to Election Day technically without aggregating the summary totals or publishing the results. For example, the county cannot pre-scan ballots before Election Day at 7:00 AM. While the Executive's recommended system is not yet certified to pre-process ballots either, the assumption is that it will be certified before the election.

Pre-scanning of ballots is not a requirement to transition to vote-by-mail. In addition, pre-scanning creates a potential source of insecurity. To address security concerns, the proposed vendor states that its technology will not "tabulate" ballots without the authentication of two people. The vendor's security procedure is not a sufficient barrier to "sneak peeks" or the theft of early results and may need to be strengthened for two reasons.

- First, as envisioned only two people would need to collaborate in order to achieve early access to election results. Compromising one or two election employees has happened in other jurisdictions.

- Second, the machine will have the data on its hard drives, and election results could be displayed from this data subtly so that only an informed individual would be able to know what the results are without having to run any report. For example, a compromised tabulation server could use colors or indenting to communicate election outcomes to the systems user without others who are in the room knowing that the information is being illegally obtained. In general, proving that a computer is not leaking information is believed by security experts to be a tough, open research problem.

Evaluation of Executive Recommendation

We evaluated the Executive's recommendation based on the following five criteria:

1. Standards Compliance: is the system certified by the federal or state governments;
2. System Operations and Growth Capability: does the system operate effectively and have the ability to meet growth in the number of voters;
3. Implementation Considerations: are there potential issues with the system if implemented;
4. System Cost; and
5. Vendor Performance.

Standards Compliance

The Executive recommended technology is not certified, either at the state or federal level and, therefore, is also not certified to "pre-process" ballots.

System Operations and Growth Capability

There is currently no track record for the Executive recommended software. With regard to the scanner hardware, we requested a complete list of all elections in which the technology had been used, but the maker, DRS, did not provide the list. The one U.K. election official we were able to identify was interviewed and described both good and bad experiences with the technology, but he had not used it in a vote-by-mail election. We were not able to determine if the hardware is capable of efficiently scanning hundreds of thousands of ballots that have been folded and mailed by interviewing the one election official we were able to reach.

Implementation Considerations

The proposed system includes other components by the same vendor currently used by the county, most notably the voter registration system (DIMS) and the server (GEM) technology. However, the accessible voting unit design for the voter-verified paper trail could allow an individual to discern the order, and, therefore, how one voted.

System Cost

The capital cost to the King County taxpayer of this acquisition in the near-term is essentially zero, because it is paid for out of a federal grant. There will, however, be substantial staff costs in the acquisition, transition, training and roll-out of the system. All

these costs would be unrecoverable should the system fail to obtain timely certification or fail.

Vendor Performance

Outside of Washington and large all-mail elections, the Executive's recommended vendor has a very large, installed base and a great deal of election experience. However, the vendor has had some negative public perceptions regarding trust, as well as a documented track record of less-than-stellar customer service and election-security practices. This vendor also does not have as much experience with tabulating high-volume, mail-ballot elections, although they have experience in mail-out of ballots for high-volume elections. This vendor also has a documented track record of less than stellar customer service and election security practices. This vendor does not have as much experience with tabulating high-volume mail ballot elections, although they have experience in mail-out of ballots for high-volume elections.

Alternative Courses of Action

We evaluated the following three alternatives to the executive recommendation for a ballot tabulation system:

1. Acquire Hart InterCivic Technology.
2. Perform Full Request for Proposal (RFP) with Commercial Vendors Only.
3. Perform Full Request for Proposal (RFP) but Include Shared Development (Open Source) Vendors.

Similar to the method used to evaluate the Executive recommendation, we evaluated each of the three alternatives based on the following five criteria:

1. Standards Compliance;
2. System Operations and Growth Capability;
3. Implementation Considerations;
4. System Cost; and
5. Vendor Performance.

Alternative One: Acquire Hart Technology

The Executive's business case considered the alternative of acquiring Hart's InterCivic technology for central scanning of ballots and ballot adjudication. Our assessment below is of the vendor's proposal as described in the Executive's business case which does not include any major upgrade in security practices or security education. In summary, the Hart technology is certified and was rated highly in the Executive's business case.

However, the Hart alternative is described in the Executive's business case to be more costly than the Executive's recommendation on the basis that moving to Hart would require retiring and replacing the Diebold accessible voting units.

Standards Compliance

The technology is in use and is federal and state certified.

System Operations and Growth Capability

Hart has a tested and proven electronic adjudication capability so the efficacy of this offering could be improved and provide an opportunity for improved chain-of-custody. It is certified to perform "pre-processing" so scanning can begin before Election Day, allowing a somewhat distributed workload could and perhaps higher quality work given less intensity and stress.

It is helpful to bear in mind that the Hart solution is designed to be used with unique IDs on each ballot in the form of a voter-visible bar code. This enables several helpful security features, such as preventing double counting. Placing unique identifiers on ballots does not meet county policy if it allows a particular ballot to be linked to the individual voter who cast it. However, there are many counties that function using this technology without having unique IDs on the ballots, including all the Hart customer counties in California.

Implementation Considerations

Moving to a new ballot tabulation system is going to involve some transition challenges. There is risk of system failure to make this transition before the 2008 presidential election, given the size of the upcoming election and given that there are no low-volume elections in which the county can test the technology and address any shortcomings identified with special procedures. The current ballot tabulation technology with new procedures could be able to tabulate the 2008 elections at lower risk of system failure than a new solution can.

System Cost

While we were not able to obtain the complete costs, the information provided does suggest that the move to Hart might be more expensive than staying with the executive's recommended vendor (DESI). This assumes that moving to Hart requires replacing all the accessible voting units rather than move to a blended approach. There would also be substantial staff costs in the acquisition, transition, training and roll-out of the Hart system.

Vendor Performance

The Executive's business case rated Hart higher than the Executive's recommended vendor based on customer service. Customer service can be a critical accuracy and security issue when timely attention is required in the middle of an election cycle.

Alternative Two: Perform Full Request for Proposal with Commercial Vendors

Under alternative two, we analyzed the option of performing the typical request for proposal process using commercial vendors. We discuss below the attributes of moving forward in using a conventional request for proposal process which does not include security upgrades. This practice would differ from the less formal request for proposal process conducted by the Executive in that:

- All the relevant vendors would be encouraged to submit proposals.
- The process would not need to be expedited.
- All options would be fully evaluated, including the status quo option of not acquiring new elections equipment at this time.

Standards Compliance

Given sufficient time, all vendors could achieve certifications for their offerings.

System Operations and Growth Capability

An RFP process that only includes commercial vendors will likely not empower the county. The next upgrade will be expensive and there will likely not be federal money to pay for it.

Implementation Considerations

Any switch away from the executive recommended vendor (DESI) will have re-training costs associated with it. It may be unwise to make any such transition before the 2008 election is complete.

System Cost

A fair but aggressive competitive bidding process could be able to save money and/or get more or better products and services. The elections administration staff are, of course, in an awkward position when negotiating with DESI, given that the vendor is their only practical source of certain types of support. An internal or consulting purchasing team would be in a better position to bargain "hard" and obtain an improved deal for the county. As with any acquisition of new technology, there will be some staff costs in the acquisition, transition, training and roll-out of the system.

Vendor Performance

Presumably, a broadly advertised request for proposal process would attract commercial vendors with a documented reputation of high customer services and responsiveness.

Alternative Three: Perform Full Request for Proposal and Include Shared Development Vendors

The third alternative would be an RFP process that includes the possibility of shared-source (open-source) development.

By a Shared Development Vendor, we mean a company or consortium of firms willing to build the election software that King County desires, get it certified federally and by the state and then, provide services including training and phone support under contract. The software would be released under a license allowing other counties to use the software.
Most importantly, the certification itself would be available to be shared with other counties using the hardware and software.

We believe that there are a range of vendors who would be interested in shared development of elections software, including some large firms that sell commodity scanning and computer technology. An arrangement could be structured so that, should the shared development vendor fail, the county would still have resources to move back to a commercial vendor. In this way, risk can be limited relative to a conventional software development process.

On the downside, because Open-Source / Shared Development solutions are not available at this point, there will be a delay for them to be produced, tested and certified. If King County were to choose this alternative, the plan would have to involve assisting the selected organization with its requirements analysis. This is a cost relative to deploying an off-the-self solution, but it provides the opportunity to provide desired county functionality.

Standards Compliance

There are no completed shared-source voting systems suitable for use in King County. Suitable systems could be built and certified for elections before the current system would need to be retired.

System Operations and Growth Capability

An RFP process that only includes commercial vendors will likely not empower the county, because the next upgrade will be expensive and there will likely not be federal money to pay for it. Systems based on commodity hardware and open-source software would be affordable post-HAVA funding.

Implementation Considerations

Being the lead jurisdiction on a shared source initiative would mean that King County would get a system designed for its very demanding needs. However, there would be some additional work specifying the system and providing developer feedback and the

system would neither be available as soon or as mature as some commercially developed systems.

System Cost

A Shared Development approach could provide short and long-term affordability. Initially, the cost of development would be in line with the cost of commercial solutions, or less. Medium and long term, costs could be much less as commodity hardware costs a small fraction of special-purpose voting system technology and the software would be essentially free thereafter. A shared source offering could be structured so that King County resources would not be put at risk in that payment would be made for progress rather than upfront. This sort of work could be solicited under a fixed-price arrangement with little outlay of money from the county until the software achieves certifications and passes acceptance testing. As with any acquisition of new technology, there will be some staff costs in the acquisition, transition, training and roll-out of the system.

Vendor Performance

A vendor could be selected based on a track record of success, understanding of and commitment to security issues and capability to support the product. There are many firms with good track records at building security sensitive and high-quality applications. Under this option, after development and delivery of the product, the county would have more flexibility than having to rely on a commercial vendor.

Peer Security Review

Approach

Three Phases of Review

There were three phases of the peer security review of the Ballot Tabulation Business Case. All three phases were facilitated by Douglas W. Jones and Eric Lazarus.

- Phase One: The broad peer security review (via questionnaire and telephone interviews) consisted of elections experts from Washington, Florida, California and Maryland. Peers included elections officials who use very similar technology as King County and individuals who administer elections in other very large counties. This review covered questions on the overall feasibility, risk assessment, and appropriateness of the Ballot Tabulation Business Case. These reviewers were granted anonymity to permit them to provide very direct and honest feedback.

- Phase Two: The second phase consisted of four elections experts who are currently working in four different counties. This set of officials reviewed a single short questionnaire on the risk involved in making several changes to the elections system before a presidential election. We wanted to sample the perceived risk of system failure in general, not only from the tabulator specifically, because of the sheer number of changes envisioned in these business plans and other published changes underway in the King County Elections office. These reviewers were also given anonymity to permit them to provide very direct and honest feedback.

- Phase Three: The peer review panel was convened by the former Election Assistance Commission Chair DeForest Soaries and consisted of nine elections experts from Florida, Illinois, California, Texas, and Maryland. This group was empanelled specifically to answer the question about the need for an upgrade in order to be able to transition to Vote-by-Mail in 2008. Panel members were:

  Ion Sancho
  Supervisor of Elections, Leon County, Florida

  Thomas "TJ" James
  Election Systems Manager, Leon County, Florida

  Pamela A. Woodside
  Former Chief Information Officer, Maryland State Board of Elections

  Patrick F. Gill
  Auditor, Sioux City, Iowa

Process

Below is the process employed for the peer security review:

1. A list of questions was generated. The questions included areas of concern from security experts, county election officials, members of the election integrity community and Councilmembers and their staff.

2. Panel reviewers were identified. We identified about 40 election officials (including former officials) with the appropriate knowledge, skills and willingness to fully participate in the review.

3. In phase one, nine reviewers answered the standard list of questions .

4. In phase two, four of the reviewers reviewed a single set of questions on the risk involved in making several changes to the elections system before a presidential election.

5. In phase three, nine reviewers answered the question about the need for an upgrade in order to be able to transition to Vote-by-Mail in 2008.

6. We wrote this peer security review report summarizing the reviewer's answers.

Phase One: Survey Questionnaire

Summary of the Questionnaire's Two Main Issues

The majority of the phase one reviewers felt the business case was well-written and organized. However, the phase one reviewers were split on whether the Executive recommendation is the best approach.

Upgrade Urgency

The peer security review was split on the need for and urgency of an upgrade to the ballot tabulation system. On the questions, we got both positive and negative answers.

On the positive side:

- *"best choice for the County"*

- *"It is also highly critical that King County replace its 10-year-old system for ballot counting. This would be necessary in any event because any technology that is 10 years old is in need of upgrade or replacement and the growth of King County into the future dictates the need for a new election system. The key issue for King County as they transition to all mail voting is to have the physical location, technology and the staff in place to be successful in that transition. It is imperative that what ever system they select to process ballots, the facility, the technology and the staff must be in place to accommodate the processing and*

tabulation of ballots through a process that ensures that all ballot received by midday on election day are tabulated on election day and that all valid ballots received after midday on Tuesday (election day) and Wednesday and Thursday and Friday of election day week be processed and tabulated by close of business on Saturday of election day week. This can be accomplished with a new ballot processing system that allows for electronic ballot duplication as part of initial and final ballot processing and for tabulation processes that are quick accurate and formatted in a meaningful way on election night.... In order to gain efficiencies from the conversion to all mail voting (efficiencies are primarily gained as a result of one voting system for 95%-98% of the voters with the remaining voting at regional voting centers) it is necessary to have one compatible system of elections and voter registration. One system provides for ease in establishing regional voting centers, public relations efforts and voter education, in depth training of election workers working in the counting center and at the regional voting centers thereby reducing and/or eliminating processing errors."

On the negative side:

- *"After some thought it appears to me that the arguments that suggest that upgrade is essential for 2008 are not persuasive. By the way, we use exactly the same equipment in my county and have since 1992 so I am very familiar with many of the issues. We anticipate that we will be able to use this technology for at least another decade.... There is very little margin for error in the plan in this business case. It is always better to develop secure and trustworthy procedures and then evaluate technology once those processes have been tested."*

- *"Is it really necessary to purchase new equipment now when there is very little time to implement a new system, particularly one that has not yet been certified? Might it be more prudent to put off the purchase until after the 2008 Primary Election [sic.- we assume that this official meant the general] and take more time to let the vendor obtain certification, plan for the implementation and transition, and implement in an orderly fashion?"*

- *"Most apparently not considered are options that preserve the status quo – the environment that the elections staff are used to working with and within – for the Presidential year, the highest volume (and thus, highest risk) year in the 4-year election full cycle. With staff already trained using current equipment and procedures, the lowest risk option is to put off major changes until after November 2008. Ignored (or, at least, completely unmentioned) is the fact that the HAVA funding is not use-it-or-lose-it this fiscal year. King County could easily say – "The Presidential year is no time to be making drastic equipment changes," and backburner all or part of the purchases recommended until the following year, 2009. This would give an opportunity for more equipment options to be considered.... If a jurisdiction's current equipment is completely worn out, or violates a law, then upgrading the technology may be the only option. This is not*

the case with King County, however. They clearly have equipment that can be used in the Presidential election in 2008, as it has successfully been used in the 2000, and 2004 presidential elections. It is a known quantity."

Request for Information Process

While several peer reviewers were impressed with the presentation of the business case for tabulation, a couple of the reviewers were concerned that the county conducted an informal request for information (RFI) process rather than a formal request for proposal (RFP) process:

- *"I would only use an RFI to help educate myself and my staff to enable us to design a good RFP."*

- *"I question why an RFI was done instead of an RFP (Request For Proposals) where more vendors could participate? Why does the Project Plan include a task for developing a "Sole Source Justification? One can infer from this that the existing vendor was going to be proposed all along."*

Phase Two: Change Risk and Management

Several election officials we spoke to formally and informally expressed concern about the tight time frames and number of changes involved expressing that they thought it might be risky.

For that reason, we developed a "phase two" of the peer review. In phase 2, four reviewers were asked questions about risk and all expressed concern that it was not best practice to make multiple large changes for Elections at the same time. Specific concerns were:

- Overwhelming numbers of voters showing up at voting centers.

- A new signature verification system may become a bottleneck the first time it is used for a sizeable number of voters.

- Mismatch of signatures on ballot-containing envelops relative to the signatures on file for that voter.

- Infrastructure breakdown including power failures, network failures, etc. in the new building.

- Problems with the new tabulator hardware, including that it might be slow or jam often when used against real ballots, and

- Problems with the new tabulator software, including with integration with other election technology.

Phase Three: Is New Technology Essential to Move to All Vote by Mail?

In phase three of the peer review, we formed a special peer panel to answer the specific question "Does All-Mail-Voting require a technology upgrade or would it be just as wise or wiser to continue to use the existing technology in the 2008 election cycle?" There are many technical issues involved with the hardware and software so it made sense to select people with deep understanding of the technology because of year of experience using it.

The unanimous conclusion of this special panel was that the current equipment owned by King County is fully sufficient to handle an all-mail election for a million voters, even in a Presidential election high-volume year, without a technology upgrade.

An Additional Option Is Available

The expert review of the ballot tabulation business case recommended that the county consider an open source alternative. *(See page 20 of this report for a description of this alternative.)*

We asked several of the reviewers their opinion about the practicality of the open source alternative and they thought it was worth considering the alternative about the open source option. Some of their comments follow:

- *"Building and open sourcing technology is not considered nor is holding off and waiting for the next generation of technology to be available. Waiting for this generation of technology to mature, seeing it work in sizable jurisdictions before adopting it in King County does not seem to be considered."*

- *"It would make sense to include companies willing to develop and then open-source license the technology if the timeline for implementation was 12-18 months. This new technology would take time for the vendor to develop and get certified at the federal and state levels."*

- *"Open source software will be the wave of the future in election administration, as the public becomes more educated and sophisticated in how their elections are actually conducted, and begin to demand the use of systems and equipment that is understandable to a layperson and as transparent as possible. Ignoring the fact that the public may be demanding the removal of corporate proprietary software from the election process within the next ten years or so is failing to recognize one of the more earthshaking, yet probable, major changes to election administration within the next ten years."*

Glossary

Adjudication Workstation – The term used in Diebold's quote to refer to computers configured to be able to alter the votes as read by centralized scanners. The function of ballot adjudication is to address the fact that a substantial percent of ballots do not scan successfully.

Automatic Routine Audits (ARA) – A security and error-detection measure used in many places, most famously, every county in California where state law has required at least a 1% hand count for many years. An ARA is believed by many security experts to be the only practical way to assure the voting public of accuracy when ballots are electronically captured and/or counted ballots. See: security and error-detection measure used in many places, most famously, every county in California. There state law has required at least a 1% hand count for many years. An ARA is believed by many security experts to be the only practical way to assure the voting public of accuracy when ballots are electronically captured and/or counted ballots. See: "The Use of Automatic Routine Audits (ARA) for Mail Ballots."

Ballot Adjudication – Voters make mistakes. It is not be uncommon for 10% of vote-by-mail ballots to not scan successfully without election worker intervention. This can be for many reasons including that a voter might put an X or a check mark instead of filling in an oval on the form. Some localities "enhance" ballots by making marks or apply clear tape and making repairs on top of the clear tape. In King County Ballot Adjudication is performed by so-called Ballot Duplication, i.e., a by hand (and, perhaps in future, electronically) entire ballots are recopied by election workers, correcting mistakes, ideally, according to procedures in force.

Red Team Exercise / Intrusion Test – Tests of a system designed to learn about the security of a system for example see if its security can be defeated, if procedures are being followed and to discover new attacks that should be guarded against. "Ethical Hacking" is an informal term used to refer to intrusion against electronic systems including computers. This term would not apply to an intrusion test done on the physical security of a building, compound or location.

Malware - Any unauthorized, undesirable functionality that finds its ways into any computer system.

Trojan horse - A program that installs malicious software while under the guise of doing something else.

Electronic Ballot Adjudication - Ballot Adjudication (voter intent ascertained) on a computer screen rather than directly on the ballot.

Shared Development Vendor – An open source developer of technology. A company or consortium of firms willing to build technology, get it certified federally and by the state to run on affordable commodity hardware and then, if desired, provide services including training, phone support, etc. under contract. The software would, thereafter, be released under a licensed which would mean that it would be available for use in anywhere.

Appendix One: Qualifications

Our team is comprised of Eric Lazarus and Douglas W. Jones.

Eric Lazarus

Eric Lazarus is a Computer System Architect and expert in many technology disciplines. He is a researcher in the area of threats and risk evaluation and mitigation in general with a focus on voting security. He was the Principle Investigator on the Brennan Center for Justice study of voting system security and the initiator of the work on voting technology performed there. His methodology has become the standard for review of voting system vulnerabilities in the context of real elections.

Eric Lazarus was the Principal Investigator of the Brennan Center Report which pioneered the methodical analysis of threats to voting systems and the power of countermeasures to address them. Eric is a co-author of an upcoming book based on the Brennan Center Report from Academy Chicago Publishers.

Eric is a co-Principal Investigator of a project to develop a repeatable, and software supported, method for rational allocation of security-related resources. Eric is also developing a unique threat-analysis application, AttackDog, which is funded by the National Science Foundation.

Douglas W. Jones

Douglas Jones is an associate professor of computer science at the University of Iowa. He was a respected member of the team that developed the Brennan Report. He helped lead the NIST workshop that was a key element of the research process.

Doug Jones served on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems from 1994 to 2004, and chaired the board for three terms. This Board examines all voting systems offered for sale in the state of Iowa to determine if they meet the requirements of Iowa law. Jones was invited to testify before the United States Commission on Civil Rights on evaluating voting technology for their January 11, 2001 hearings in Tallahassee Florida. He was invited to testify before the House Science Committee on problems with voting systems and the applicable standards for their May 22, 2001 hearings. He also was invited to testify before the Federal Election Commission on voting system standards for their April 17, 2002 hearings.

Jones wrote Chapter 1 of Secure Electronic Voting, edited by Dimitris Gritzalis and published by Kluwer Academic Publishers in 2002.In the summer of 2004, he consulted with Miami-Dade County to assess problems with their touch-screen electronic voting system and to assess their pre-election testing of their touch screen and optical scan voting systems. His paper, Auditing Elections, was published in the Communications of the Association for Computing Machinery in October 2004.

Doug Jones is one of the ten principle investigators in A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections (ACCURATE), a multi-institutional center awarded a 5-year research grant by the National Science Foundation starting in October 2005. He has special expertise in the evaluation of optical scanners, the core of nearly all modern vote-by-mail systems.

Appendix Two: Review Limitations

There are several sorts of information we would have expected to be able to get as part of a security review which we were not supplied.

- Diebold has not provided information about how the scanner hardware, from UK firm DRS, has functioned in the past and did not provide us contact information for customers in Europe who have used the hardware component of their offering.

- Diebold has not provided accuracy figures from their own internal testing. Diebold agreed to share those with us but, as of yet, we have not received it.

- Many of the security features described by Diebold could function have limited value and, but we have not been able to get details on them or on how they function to address any specific attacks.

- While Diebold representatives stated in a meeting that they never prevent anyone from doing security testing on their technology, we have received from elsewhere a contract that Diebold signed preventing another election jurisdiction from performing security testing under threat of voiding all warranties.

- Diebold was not willing to supply manuals describing the operation of the new central scanning solution we were attempting to evaluate.

- The senior project manager and lead developer we spoke to were not aware of any red-team intrusions testing exercises planned or executed against the technology and while they assured us that Diebold had taken up security with new seriousness and dedication, they have yet to supply this information.

There were other challenges with regard to this analysis, including:

- The Executive informed us that they have not determined what procedures will be used with these technologies. Some of the procedures could have implications for security in general and transparency in particular. For example, both procedures for auditing and for recounts are highly sensitive to the details of the technology. They have large implications for the security of the overall election. Procedures to ensure that electronic adjudications were performed correctly are likewise critical to assessing security.

- The Executive stated that they have not negotiated contract terms and that they currently do not plan to begin to negotiate until after the King County Council has determined who the vendor will be. A best practices pre-purchase security review such as this one would generally examine contract language looking for such items as vendor commitment to rapid repair of security vulnerabilities once discovered and reported, as well as the contractual commitment to support security investigations without onerous restrictions. We were not able to perform this entire section of the security review.

- The Executive has not explained how king County Elections plans to audit provisional ballots captured onto the Diebold TSx machines. These machines are not state certified currently for this function.

Appendix Three - Observations Relevant to Diebold Election Systems Inc. (Diebold) and Election Security

Many recognized security experts have been uncomfortable with Diebold as an election system vendor based on their historical track record.

We focus in this section on Diebold, not to unfairly chastise them above other election vendors, but because the RFI process the county used in place of the more risk adverse RFP process normally used for technology purchases of this size, produced a result that was heavily Diebold-dependent for success, and thus the security of the business case must be evaluated in that context.

While the following incidents are worrying, it is not the case that security experts generally assume that the other commercial vendors have a far higher commitment to security than does Diebold. The big vendors are all selling their products to county-level election staff, very few of which have the resources to evaluate system security, so there is not much reason for a commercial vendor to invest heavily in security, beyond the minimum required to achieve state and federal certification. The 1990 voting system standards for security were weak, and newer standards, although stronger, have not corrected all of the problems in the earlier standards. This fundamental problem suggests the wisdom of moving toward open-source voting technology.

It does appear to be the case that, as the market leader, Diebold has been investigated more often than its competitors and this should be taken into account on balance. Further, it should be noted that DESI (Diebold Election Systems, Inc.) was an independent firm, Global Election Systems, until acquired and day to day operations were taken over by Diebold late in 2002. Some of the problems were uncovered or at least germinated before Diebold, a venerable name in banking equipment, acquired the company.

On Nov 6, 1997, Doug Jones, co-author of this study, was reviewing technology from Global Election Systems, the firm that would become Diebold Election Systems, as part of the first Iowa examination of the AccuTouch system. He wrote, "It came out that neither the technical staff nor salespeople at Global Election Systems understood cryptographic security. On continued questioning, it became apparent that there was only one [encryption] key used company wide for all of their voting products. The implication was that this key was hard-coded into their source code." Doug warned the vice president of the then Global Election Systems that this practice was unacceptable and in fact, provided almost no security.

On July 24, 2003, Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin and Dan S. Wallach released a report on their examination of unencrypted code that had been recovered from Global Elections' web site very shortly after the acquisition by Diebold was complete. This paper has become known as the Hopkins Paper. It makes it clear that the errors Doug had pointed out to representatives of Global Election Systems when they first came to Iowa with the AccuTouch system had not been corrected in the source code that was available on Global Elections' server five years later.

On January 20, 2004, a study commissioned by the State of Maryland was released. Titled "Trusted Agent Report: Diebold AccuVote - TS Voting System" it describes a red-team exercise (that is an attack or intrusion performed to test a systems security) which resulted in the discovery of many security vulnerabilities of significant concern. For example, the study says: "The GEMS server lacks several critical security updates from Microsoft. As a result, the team successfully exploited a well-known vulnerability using a common commercial software product known as Canvas. This vulnerability, described in a security advisory from Microsoft for which a patch was made available on July 16, 2003, allows a remote attacker to get complete control of the machine. Since this is the same weakness that the August 11, 2003 "Blaster" worm exploited, it means that if the GEMS server was exposed to an environment where "Blaster" was propagating, it might have been infected. By successfully directing Canvas at the GEMS modem interface, the team was able to remotely upload, download and execute files with full system administrator privileges. All that was required was a valid phone number for the GEMS server." (As we understand King County's setup, the GEMS servers currently have no phone or other modem, a very important security measure.)

In April 2004, the California Secretary of State, Kevin Shelley, determined that the software in use on Diebold touch screen machines in its counties was not certified at all. According to the staff report: "...Less than a month before the March Primary, after repeated assurances to the contrary, this office learned that Diebold was no longer pursuing federal ITA approval of the software and firmware installed on California voting machines. Rather, Diebold had instructed the ITA to test a newer version of both software and firmware. It also became clear that the federal ITA could not approve the newer software and firmware before the March Primary." This put the state and its counties in a very difficult position.

"On July 20, 2005, 96 Diebold TSx DREs with AccuView printers machines were tested by the [California] Secretary of State's office over a period of 5.33 hours in a setting designed to emulate a real election. This appears to be a first: as far as we are aware, no controlled test of this scale has ever been performed before anywhere. This provides an opportunity not only to assess the reliability of the TSx, but also to examine the effectiveness of volume testing in general." According to the report *Analysis of Volume Testing of the AccuVote TSx / AccuView*, "We found that there were 34 failures, spread across 29 distinct machines. We classified each failure into one of two categories: (a) printer jams, and (b) software failures, where the touchscreen machine crashed, froze, hung, or reported an unrecoverable error condition. The 34 failures broke down into 14 printer jams and 20 software failures, with 12 machines experiencing at least one printer jam (2 machines suffered from 2 printer jams) and 18 machines experiencing at least one software failure (2 machines encountered 2 software failures). One machine experienced both a printer jam and a software failure." This is ten times the acceptable rate of failure according to national standards.

In December 2005, Hugh Thompson of Security Innovation and Harri Hursti, a Finnish computer scientist, were able to change votes on the Diebold machine without leaving evidence that they had done so. (This is one of the vulnerabilities that is the focus of the Emmy nominated HBO special "Hacking Democracy.") The vulnerability involves software design choices that are not conventional in systems designed with security in mind.

In July 2006, Black Box Voting released a report which described remarkable vulnerabilities in Diebold technology analyzed by Harri Hursti and others, among them that "the Diebold boot loader for the TSx release seems to contain the full capability to "reflash" (i.e. update) itself and the operating system." What this means is that the same model of touchscreen voting machine that King County acquired once was released with a program that would allow new software to be loaded, replacing any or all of the software the machine came with, including the voting system software or the operating system that controls all the operations of that terminal. The implication of this is that anyone who has access to the memory cards that will be installed in machines can control the behavior of those machines. The machine that performs ballot definition functions, i.e., the GEMS Server, becomes an important point of vulnerability as that machine places the data onto the memory cards that can, thereafter, take over the voting terminals.

Despite Diebold's historical record of failure to apply best practices for security with their voting machine equipment, the company claims that their commitment and capability with regard to security are good now and should be acceptable to any municipality.

After all of the public attention to security problems with Diebold's products, we expected Diebold to make effective changes, but on July 16, 2007, a group at the University of Connecticut released a report on *Integrity Vulnerabilities in the Diebold TSX Voting Terminal.* In this report, they showed that the memory cards used on the TSX remain vulnerable despite Diebold's use of cryptographic protection on those cards. In effect, it is fair to conclude that cryptography was used incorrectly in the design of this system.

We asked for and, in our view, did not receive concrete evidence of a major shift in priorities toward improved security. We received many assurances but little evidence that change had taken place. While the system of federal testing has been upgraded in that labs are far better monitored than in the past, the standards to which these labs test remain weak. As such, one should not expect to see certification motivating much in the way of security improvement in the near future.

Appendix Four: Additional Security Issues

Security Isn't Just Passwords, Locks & Keys

Achieving excellence in security requires enhanced knowledge, skills, commitment and dedication on the part of elections management and staff. Below, we provide detailed examples of ballot secrecy issues to illustrate the value of a comprehensive rethinking of security in King County elections.

This is important to note, as acquisition of new technology will not automatically address many of the deviations from best security practices in King County, and may well serve as a distraction from repairing them.

Election security is measured in two principal dimensions:

1. Integrity of the count, the resistance of the election system to clerical error or manipulation.

2. Ballot secrecy, the extent to which the election system protects voters' right to privacy in voting choices, which in turn, prevents voters from facing reward or punishment on account of how they voted.

These two requirements sometimes come into conflict. For example, a show of hands in a closed meeting room has very high integrity. Every participant can independently count the votes and determine whether the result announced from the front of the room is accurate. In exchange for this, a show of hands completely sacrifices ballot secrecy. Every person in the room must reveal how they voted to everyone else. In so doing, they set the stage for a variety of vote buying and voter intimidation attacks on the election.

Vote by Mail Batch Ballot Secrecy Risk

In the case of absentee, postal, or "by mail" voting, one important component of election security involves the size of the batches in which the ballots are tabulated.

Absentee, Postal, or Vote by Mail ballots (hereafter called VBM ballots) are tabulated in batches for many reasons. Processing ballots in batches that can be completed in one work shift with the same staff and observers, and maintaining separate accounting for each batch can minimize errors. This procedure allows integrity checks to be applied to the processing and tabulation of each batch of ballots.

However, there is a risk of losing ballot secrecy here: If the batch size is small enough and there are enough distinct precincts and/or ballot styles, then some of the ballots in the batch will be the only ballots from their precinct or ballot style. If we know which voters' ballots went into a batch, and if we know the vote totals for the batch, we can uniquely identify the votes of some voters. Specifically, if a voter was the only representative of their precinct included in a batch, the voter's votes on any races unique to that precinct or split will be thus publicly disclosed.

Note that our goal of providing an absolute guarantee that nobody can discover how any particular voter voted is, strictly speaking, mathematically impossible. For example:

- If all the voters in some particular batch vote identically, we know how all of them voted.
- If an election is unanimous, we know how everyone voted.

These situations are extraordinarily unlikely, and they are cases where the information disclosed is not very socially threatening, as the voter has voted identically to all of their neighbors, or the entire jurisdiction.

The information we learn in these cases is that a voter voted with the majority. In general, disclosing a voter's vote is at its most dangerous if we disclose that the voter was in the minority, and it is at its most dangerous when that minority is small or singular. The one voter who voted against a landslide is the one who needs the greatest protection.

Vote by Mail Batch Ballot Secrecy Solutions

How can we protect ballot secrecy from this class of attacks? One answer is simple: King County sorts VBM ballots by legislative district. If we pre-sort as much as possible down to the precinct level, which was once standard practice in King County, the percentage of voters whose privacy is threatened approaches zero.

In sum, the more finely ballots are sorted prior to batching for tabulation, the smaller the threat to ballot secrecy posed by any release of batch totals. Note that perfect sorting is not required. We do not need to sort down to the individual ballot style to achieve a useful degree of privacy, and we do not need to raise the batch size to anything unmanageable.

Provisional Ballot Canvass Ballot Secrecy Risk

Let us examine an example where ballot secrecy could be violated in King County. An example, is when a citizen's voting choices are revealed because their party affiliation differed from the large majority in their precinct. This is a classic example of a voter in the minority party needing protection. A solution to the problem is to have the data from the provisional ballot in the precinct combined with the poll ballots in the canvas file. In this way there would be a large enough number of votes to obscure one's voting preference.

Provisional Ballot Canvass Ballot Secrecy Solution

We have been informed that previously, the standard procedure in King County was to combine the provisional ballots cast by poll voters with the poll ballots from the voter's precinct, and the provisional ballots cast as absentee ballot replacements with the absentee totals of the precinct. This a procedure that should be reinstated.

On-line Ballot Tracking Secrecy Risk

There is another reason to be concerned. Many election jurisdictions, including King County, are moving toward systems where voters can inquire, on-line, to determine the status of their VBM ballots. A citizen intent on selling their vote need only give the vote buyer their ballot tracking number in order to allow the vote buyer to learn exactly when that ballot was stripped from its envelope.

Knowing this exact time should suffice to allow the vote buyer to identify the batch into which the ballot was placed. Working from the other side, public accountability makes it natural to demand that all batch totals be made publicly available to anyone wishing to check the county's arithmetic. The net result of combining these two sets of considerations is to defeat the voter's right to a secret ballot.

On-line Ballot Tracking Secrecy Solution

The date of ballot receipt and validation, and not the exact time, should be the only information placed on the internet. This is acceptable transparency to assure the voter that their vote was received and accepted for tabulation.

Ballot Secrecy and the Opening Process Risk

Ballot secrecy also depends on how the envelopes are opened. In our observation of VBM ballot processing in King County, we noted that incoming envelopes were batched prior to opening, and that a single election employee opened the outer envelope, then removed the ballot from the inner privacy sleeve and inspected the ballot to insure it would likely scan correctly. While that worker is instructed to open all outer envelopes in a batch before opening the first inner envelope, and then opens all inner security envelopes before inspecting the first ballot, it is still possible for an individual worker to remember that, for example, a particular famous person was 10th in the stack and then remember how that person voted.

This is not a best practice as it allows an election department employee to see how some voters have voted and we recommend that King County avoid any similar procedure.

It is our understanding that King County Elections once used an assembly line process: one employee to open the outer envelopes, and a second employee to open the inner envelopes, and a third employee to examine the ballots for stray marks that would impede tabulation and place the ballots in a box, ready for proceeding. At some point, this practice was changed in order to speed ballot processing.

The double envelope model permits a strict separation of functions, where the ballot is not removed from the inner privacy sleeve until the link with the outer envelope has been irrevocably broken. The voter has a reasonable expectation that ballot processing will be used this way.

Ballot Secrecy and the Opening Process Solution

King County should return to their previous practice of using multiple employees for ballot opening, and irretrievably breaking the link between the ballot and voter identity, before the ballot is removed from the security envelope.

Ballot Assembly and Mail-out Risk

One way to model the threat is to assume that voters are selling their votes to a vote buyer who is in a position to extract some kind of penalty from voters who accept a payoff and then fail to follow instructions.

Consider a typical penalty imposed by a classic urban political machine: You will lose your patronage job if you do not vote as instructed. What risk would a typical member of the political machine be willing to take? Would you vote against the machine if you had a 37% chance of being caught by the machine's enforcement squad? How about a 2% chance? If we sort the ballots so that no more than 50 ballot styles may appear in any batch of 200 ballots, we come close to 2%. If we allow no more than 40 ballot styles per batch, batches of 200 ballots will threaten fewer than 1% of the voters.
Special Integrity Issues Raised By Vendor Mail Ballot Handling

The above discussions of sorting ballots into batches need for a significant amount of bulk mail processing equipment. Such equipment is expensive, and when an election is not in progress, the County has no use for such high-end mail handling equipment. This strongly suggests the value of hiring a bulk-mailing contractor.

Both ballot mailing and returned ballot sorting are security critical tasks. A corrupt individual involved with ballot mailing could easily arrange not to mail ballots to precincts with record of favoring the wrong party or that are, based on demographics, undesirable.

> **Possible Scenario**: Given an appropriate match between data from pre-election voter surveys, it would even be possible to selectively fail to mail ballots to voters who show up on surveys as being undesirable. Even a 5 percent cull rate within such precincts would potentially alter an entire election. To maintain the expected postage bill,an individual could easily apply new address stickers and mail the ballots to a PO box under their control.

Attempts to identify which voters did not get ballots and to correct the problem are very difficult. Certainly, some voters will notice and complain. In every election in King County, many voters claim they did not receive their ballots, most the victims of the normal rates of lost and mis-delivered mail, who ask for replacement VBM ballots or provisional ballots. It is safe to assume that some voters simply choose not to vote, rather than correct the problem.

Ballot Assembly and Mail-out Solution

Simply relying upon voters to complain about ballots that have never been delivered is an insufficient safeguard against deliberate or accidental missed deliveries of VBM ballots.

If a contractor is used for ballot printing, ballot mailing, or for any stage of return ballot processing, there must be some way for election observers to monitor the operation of the contractor. Ideally, all ballot processing done by contractors should be just as accessible to observers as ballot processing done by the county. Buying or leasing mail-processing equipment and using it centrally on county premises with observers, as was done in the past in King County, has substantial security benefits over shipping ballots to sorting facilities.

How Much Privacy is Enough?

It is reasonable to ask, how much privacy is enough? Since we cannot achieve perfect ballot secrecy, for example, in the face of a unanimous election, we cannot say that any disclosure of how any voter voted is unacceptable. To cite another example, in the days leading up to the certification date of an election, late VBM ballots arrive in such small numbers that it would be difficult to safeguard secrecy for these ballots. Rather, we must take a more pragmatic approach.