RESPONSE TO REQUEST FOR PROPOSAL
VOTING SYSTEMS/EQUIPMENT
SOLICITATION # DG5502
ISSUED JULY 9, 2004

TO: Governor Olene Walker
Lt. Governor Gayle McKeachnie
Amy Naccarato
Utah Procurement

FROM:

Erik Brunvand-Assoc. Professor, School of Computing, Univ. of Utah
John Carter-Assoc. Professor, School of Computing, Univ. of Utah
David L. Dill-Professor of Computer Science, Stanford University
Kathy Dopp, M.S. Mathematics
Samuel H. Drake- Research Associate Professor, School of Computing and Dept. of Mechanical Engineering, Univ. of Utah
Ganesh Gopalakrishnan- Professor, School of Computing, Univ. of Utah
Mike Jones- Assistant Professor of Computer Science, BYU
David Hanscom- Professor, Clinical, School of Computing, Univ. of Utah
Art Lee- Assoc. Professor, Clinical, School of Computing, Univ. of Utah
Jay Lepreau- Research Professor, School of Computing, Univ. of Utah
Dow W. Patten, Esq.
John Regehr-Assistant Professor, School of Computing, Univ. of Utah
Kent Seamon-Assistant Professor of Computer Science, BYU, Director, Internet Security Research Lab
Barbara Simons, former President, Association for Computing Machinery
Pamela Smith
Dan Wallach, Asst. Professor, Rice University Department of Computer Sc ience
Phillip J. Windley-Associate Professor of Computer Science, BYU
Richard Wyman

DATE: JULY 19, 2004

I. INTRODUCTION

This document is a response to the Request For Proposal ("RFP") issued by the Lieutenant Governor's Office. The opinions and analysis contained in this response are those of the authors only; however, many of the issues raised in this response are common issues facing state elections officials throughout the country as they attempt to avail themselves of federal dollars while complying with the provisions of the Help America Vote Act ("HAVA"). These comments and suggestions are not exhaustive, and other issues or perspectives may reveal additional inadequacies in the RFP.

We strongly feel that the present RFP is an insufficient basis upon which to acquire voting machinery which will inspire public confidence. We are committed to assisting the Committee and the Lieutenant Governor in addressing the issues outlined in this response by revising the existing RFP, and setting up evaluation mechanisms in sufficient time to meet the goal of the June 2006 election. Though this response focuses on Direct Recording Electronic ("DRE") solutions, other types of solutions, such as optical scanning devices may need further scrutiny of the tallying and management technology. The state should require all electronic systems, both DRE and optical scan to retain a "ballot image" that can be used to troubleshoot the system in case of errors, and can be useful in enhancing security without significant additional cost.

Aside from the schedule, the RFP is generally good as far as it goes. However, without additional cost, and with little burden, the RFP can be made much more specific in ways that will save Utah taxpayer dollars over the five (5) year life of the contract, and will make the RFP a much clearer yardstick by which to judge competing solutions. To supplement this greater specificity it is recommended that the State use its power to have outside experts review all proposals, including the source code of electronic systems, for adherence to more specific requirements. It is only in this fashion that the public will have the necessary faith and confidence that not only is the selected system accurate, reliable, and secure, but that it is the best, most cost-effective solution for Utah.

In reviewing these comments it is useful to keep in mind that no voting solution can deliver 100% accuracy, security, or accessibility. Each of these primary goals are better seen as points upon a continuum, where constant effort and diligence is required to keep the momentum moving towards the upper percentages, rather than slipping into inaccuracy, becoming more susceptible to tampering or hacking, or diminishing in ease of use.

II. PROBLEMS AND SUGGESTIONS

PROBLEM: SCHEDULE TOO AGGRESSIVE

The stated schedule is not in the best interests of the state and its citizens. The schedule is so aggressive that the state faces substantial but unnecessary risks in the areas of cost, liability, and the security and accuracy of the voting process.

The voting equipment arena is currently in such great turmoil that delaying the acquisition process just a single year would greatly reduce the state's risks and probably its costs. Available equipment, its costs, the standards, the laws, judicial rulings, and public opinion are all in great flux. For example, the procurement does

not take into consideration pending federal legislation, such as House Resolution HR2239 and Senate Bill S1980, which have specific paper-trail requirements, nor likely standards from the EAC/NIST.

These goals are much better met by delaying the acquisition process while all aspects stabilize. It is in the interests of no one, including the disabled, to have to revisit the selection, or to be stuck with an inaccurate or insecure system by rushing in too early. Finally, as detailed below, the current schedule is far too aggressive to allow reasonable opportunity for a security review.

PROBLEM: INSUFFICIENT TIME FOR SECURITY REVIEW BY THE STATE

The schedule for selection of voting equipment gives just 17 days between bid submission and first round results announcement, an insufficient amount of time to do an adequate security analysis of the full source code and procedures. Professor Dan Wallach, a member of the team that analyzed the Diebold system, estimates a minimum of 5 person-months to audit the software for a single system-- and that is not including an audit of the operating system source code.

Because the security questions asked in the first round are not specific enough to determine if basic security requirements are met, even assuming that vendor responses are accurate, and because there are only superficial attempts to evaluate security in the second phase of the evaluation, the overall result is that security evaluation of voting machines is entirely inadequate under this RFP.

Furthermore, the stated schedule for procurement does not take into consideration pending federal legislation, such as House Resolution HR2239 and Senate Bill S1980, and rapidly changing standards. By permitting time for an independent review, the State may also benefit from falling prices for voting equipment.

PROBLEM: LACK OF INDEPENDENT SECURITY REVIEW REQUIREMENT

The RFP lacks a definite requirement for independent security review. We concur with the conclusions of the Brennan Center report, which sees a team of an independent security experts as necessary to inspire voter confidence and minimize risks. Though that report is directed to immediate use of paperless DRE machines in the 2004 election, the recommendations are relevant to the fine tuning of the RFP and promote public confidence in the selected system. The experts would evaluate every machine under consideration during phase I and the schedule should be amended to allow sufficient time for independent review to take place.

PROBLEM: NO ADDITIONAL CONSIDERATION GIVEN TO OPEN SOURCE SOLUTIONS

The present RFP does not add any points for Open Source Software solutions. Open Source solutions by their very nature a) inspire greater public confidence, as they are open for the world to review and critique, and b) due to that broad review, have a much better record of security and correctness. The scoring for the selection of the RFP should provide additional points for Open Source Systems.

PROBLEM: INSUFFICIENT SPECIFICITY IN MINIMUM REQUIREMENTS

The current RFP does not state minimum requirements with enough specificity to provide the baseline against which proposals can be evaluated. In state procurement, an RFP sets the standard to ensure that the State gets what it needs. As presently drafted, the RFP appears to invite vendors to educate the State about its needs.

For example, the RFP does not sufficiently describe human factors requirements, other than a brief requirement that the system be tested with actual voters. “Ease of Use” is far too broad a term for a requirements document. Human factors analyzes the interaction between the technology and the human using it, measuring the number, length, and qualities of user actions and how those actions are laid out and presented to the user. Human factors analysis can provide hard metrics that will enable the State to have a clear yardstick to measure the ease of use of the various proposals.

PROBLEM: LACK OF VOTER VERIFIABLE PAPER AUDIT CAPABILITY

We are particularly concerned about the lack of a requirement for voter verifiable paper audit capability in electronic solutions. The RFP makes a nod in the direction of security and says that's the second most important selection criteria (after cost), but saying you are concerned about security in general terms without being quite specific about what you require leaves the door open for all kinds of rationalization. Paper’s security risks are well known and understood. It is essential to provide a paper audit trail, verifiable by the user as a minimum requirement.

One need look no further than the constant plague of email viruses and security warnings to understand that computers suffer from a whole host of security problems. The problem is that security is not something you can guarantee with a few code reviews or a carefully chosen panel of experts (as the RFP suggests). In fact, security is so hard to achieve that most Computer Scientists who have looked at the problem have concluded that the only way to prevent problems is to ensure that you provide a method for auditing the results, provide for independent recounts

and to allow each voter to check the results of the machine. This is called a voter verifiable paper audit trail (VVPAT).

Unfortunately, when it comes to computer security, and especially in an area as important as ensuring the integrity of the voting process, you need the help of computer professionals. This isn't an area where consensus alone will necessarily lead to a better result.

A simple and effective solution which would address the vast majority of stated concerns on this issue is for Utah, through the Lieutenant Governor's Office, to simply adopt something like the California Secretary of State's June 15, 2004 "State of California Standards For Accessible Voter Verified Paper Audit Trail Systems In Direct Recording Electronic (DRE) Voting Systems." (Appendix 2). These standards specify minimum requirements in a fashion which would greatly inspire voter confidence in any solution selected by the committee and would silence most critics on the issue. Though they only apply to DREs, they are a step in the right direction. The State may want to consider defining the paper audit trail in a more or less restrictive fashion than the California Secretary of State.

The state should require all electronic systems, both DRE and optical scan to retain a "ballot image" that can be used to troubleshoot the system in case of errors, and can be useful in enhancing security without significant additional cost.

PROBLEM: DREs ARE NOT REQUIRED BY HAVA

The stated intention of the RFP is to be general and broad enough to allow for selection of any type of voting equipment including touch-screen interface to paper ballots, and new optical scan "ballot on demand" systems, that print optical scan ballots and can provide an accessible interface to the ballot-printing computer-- so a ballot can be printed with the votes already marked.

However, the RFP states: "The proposed voting solution must include at least one DRE per polling place that will accommodate persons with disabilities." The RFP already defines "VWD Unit" as a HAVA-compliant device (RFP, p. 5). The RFP should continue to use the "VWD Unit" terminology instead of "DRE".

Under customary definitions of DRE, this requirement precludes other presently available voting systems that meet HAVA's accessibility requirements, simply because they are not defined as DREs.

SUGGESTION: The RFP language should be changed to read "The proposed voting solution must include at least one voting station per polling place that will accommodate persons with disabilities" or similar language, so that the best

solution for Utah voters is not inadvertently eliminated by this language. Requirement No. 33 should be changed to VWD Unit, rather than requiring a DRE.

PROBLEM: PROPOSALS NOT EVALUATED AGAINST EACH OTHER

The selection process contains an arbitrarily large hole in a process that is apparently striving for neutrality. Each different type of equipment is being evaluated separately, instead of against all others.

"The State of Utah reserves the right to evaluate each type of equipment proposed as a solution with other like types of proposed equipment solutions. Each type or group will be evaluated independently. The State will determine which proposed solution best meets the State's requirements and will make an award based on this decision. The award may not necessarily be made to the highest overall scoring offeror. Rather, the award will go to the highest scoring offeror for the proposed solution preferred by the State of Utah."

The stated goal of cost fairness, allowing for differences in up-front and downstream costs between differing systems does not require that each system be independently evaluated. Well-accepted accounting principles allow comparisons between differing systems, based upon all costs involved, projected increases in voter rolls, and maintenance.

SUGGESTION: Break the RFP into more phases where solutions using similar technologies are compared against their peer solutions, then against all other solutions.

PROBLEM: INSUFFICIENT DETAIL ON UP-FRONT AND DOWNSTREAM COSTS

Costs for storage, transportation, set up, connectivity, physical security, cleaning, maintenance, and upgrades must be specified by each vendor. The present RFP does not sufficiently specify how those costs are to be identified and calculated.

PROBLEM: INSUFFICIENT SPECIFICITY IN SCALABILITY REQUIREMENTS

The introduction implies, but does not state a requirement that the system scale to meet anticipated population growth. This should be made specific to at least the minimum anticipated population growth over the period of the contract.

PROBLEM: NO REQUIREMENTS FOR TRANSPORTATION AND STORAGE OF DREs PHYSICAL SECURITY

The state should conduct a cost analysis for storage and transportation of voting machines. For example, DREs require a much higher level of security than machines that don't actually record the votes, because if unauthorized (or even

authorized) person were to access the code, he or she could impact the results reported by the DREs. The same is not necessarily true for optical scans and ballot marking systems.

The State uses a number of different polling places. If machines are delivered early to the polling places, each polling place becomes an area of physical security concern for the period it is stored. Furthermore, the machines are a security risk between elections. These costs are hidden costs that may not be reflected in responses to the existing RFP.

PROBLEM: EXCESSIVE DISCRETION RETAINED BY STATE

Criteria can effectively be waived or set aside at the end of the bid process. How does the State determine what constitutes "preferred by the State of Utah?" This kind of uncertainty makes it more difficult later to hold the vendor to the stated requirements because they are undocumented. Excessive discretion potentially invites litigation between the State and vendors.

PROBLEM: INCONSISTENT TERMINOLOGY

Terms: Patch, Update, Version, Firmware

These are inconsistencies which have import beyond the ordinary ambiguity of procurement. These terms have specific meanings in different contexts. For example, a “patch” implies but does not specify a system level software change. SUGGESTION: If these terms must be used, their interrelationship should be spelled out in the Definitions section of the RFP.

The manner in which a patch is applied can implicate other requirements, such as Secret Ballot. Furthermore, the the RFP should contain specific definitions of how the solution must maintain secrecy in light of software changes, among other things.

PROBLEM: ERRORS IN WEIGHTING

The RFP's executive summary says that "Next to cost, which state law requires to be weighted at 30 percent, the security and accuracy category is weighed most heavily in this evaluation." Unfortunately, that is not borne out by the numbers. A simple arithmetic analysis and categorization (see "Evaluation Percentages" Appendix 1) of the bottom line yields these weights for the ultimate decision:

50% Ease of Use and "Features"
40% Cost (and Durability and Support)
10% Security and Accuracy

The result is that a voting machine vendor could fail completely in "tamperability" or even the entire security category and still win the bid.

PROBLEM: NO REQUIREMENT OF PUBLIC SOURCE CODE REVIEW

While Public Software (software whose source the public can view, but not necessarily use) provides a high degree of voter confidence, a simple non-disclosure agreement would allow members of the public to review the source code of all submitted voting systems. Further assurances to vendors could include bond requirements supporting any non-disclosure agreement.

The RFP does not require that voting machine software be open for public review. Although the RFP does require source code to be submitted , there are no terms for when the escrow may be released. We believe that security, accuracy, and reliability of Utah's voting machines would be increased if the voting software were made public (not necessarily released into the public domain), allowing the public to know how the votes are recorded and tallied.

As detailed below, more resources and time are necessary to perform source code review of all submitted systems beyond the 17 days currently allotted.

SUGGESTION: OPEN THE ACQUISITION PROCESS TO ENSURE VOTER CONFIDENCE. ORAL PRESENTATIONS (RFP, p. 7) SHOULD BE OPEN TO THE PUBLIC, SOURCE CODE SHOULD BE OPEN TO THE PUBLIC UPON SIGNING A NONDISCLOSURE WITH ASSURANCES OR PENALTIES ATTACHED.

PROBLEM: FISCAL ISSUES, WARRANTIES, AND GUARANTEES

In the hopefully unlikely scenario in which the State must call upon the warranty provisions of its final contract, it is necessary for the State to make written notice of nonconformance to the vendor. (RFP Instructions and General Provisions, ¶ 10). Without sufficient detail in the RFP, as detailed above, it will be difficult for the State to reduce to writing any nonconformance. Similarly the wide discretion outlined above may result in a system purchase, with no ability to call the vendor to account under the warranty because the failure of the system is in an area which was not part of the requirements process.

PROBLEM: LACK OF OBJECTIVE METRICS

The RFP generally suffers from a lack of objective metrics to which the proposals must be measured. For example, the definition of DRE (RFP, p. 4) requires an audio interface, but does not supply minimum standards--metrics--which can be used as baselines, such as frequency ranges, signal to noise ratios, or other

widely accepted measurements that can define the minimum qualities necessary to achieve the State's stated goals of access and ease of use for persons with vision disabilities.

PROBLEM: REQUIREMENT NO. 9 LOGIC AND ACCURACY TESTING INADEQUATE

Requirement No. 9, Logic and Accuracy Testing raises several issues beyond those specified above relating to use of terminology and insufficient specificity. The term "accuracy" is not defined in the RFP, and it is unclear to what it refers in Requirement No. 9. Further, by limiting the logic and accuracy tests to the memory of the main processor and the programmable memory device, the RFP sets up a situation where a particular voting solution may process all the votes in other associated processors (ASICs), not the "main processor", and those associated processors would technically not be required to pass logic and accuracy tests.

The "zero tapes", which are also required in Requirement No. 9, are required to recite only the zero, the machine's serial number and the "firmware" of the device. It would be very simple to require more information on the zero tape, such as software versions and boot/shutdown logs. The more information available on the zero printout, the easier it is to troubleshoot voting problems.

PROBLEM: REQUIREMENT NO. 10 FAILURE OF THE UNIT INADEQUATE

Requirement No. 10 Failure of the Unit only requires the unit to retain all votes cast prior to the failure. Other information is easily stored along with votes, including diagnostic information similar in concept to airline flight recorders. The RFP should require further information to be stored in addition to votes cast prior to failure; such as, time of failure, final and penultimate instructions, and software keys and versions.

PROBLEM: REQUIREMENT NO. 11 UNDERVOTES AND OVERVOTES INADEQUATI

The present RFP requires the machine to be able to alert the user to an over or undervote. (RFP, p. 14). The requirement should be changed to include the capability of allowing the voter to correct the overvote or undervote before making the ballot final. Also, as stated, the text implies only DRE systems are capable of warning of an overvote, which is incorrect. The mention of DRE should be deleted.

PROBLEM: REQUIREMENT NO. 13 TAMPER PROTECTION

As discussed above, physical security of DREs at all time both before, during, and after elections is essential to guard against tampering. The RFP should be revised

to require the system to provide for security at all times rather than from turn on to turn off. The State should also reconsider the requirement of blocking access to voted ballots prior to the close of polls, as this may rule out some error detection techniques or mechanisms.

PROBLEM: REQUIREMENT NO. 28 CANVASS AND ELECTION NIGHT REPORTING REQUIREMENTS

This requirement requires the solution to print out in "various formats". The required formats should be stated. This requirement states that the proposed solution must also be able to report election night results to a website. This portion of the requirement opens the door to network access. When a solution is required to attach to a network, especially a network as insecure as the Internet, the security requirements change. The RFP should more specifically state how such election night results are reported, over what type of network, and the protocols to be used. We recommend making non-mandatory the current Web reporting requirement.

III. CONCLUSION

The State should amend the RFP to address the issues raised in this response. The State should further exercise its discretion to provide time and resources for a complete and independent review of proposals, given the present state of DRE security and reliability. The State should make the entire process as open as possible in order to avail itself of public resources, and look to share costs and form partnerships with other governmental and non-governmental entities.

APPENDIX 1 EVALUATION WEIGHTS

FIRST ROUND
In the first round, the weights are:
- 20% Security and Accuracy (Section A)
- 10% Offeror's Ability to Support System (Section B)
- 15% Election Management (Section C)
- 15% Ease of Use and Accessibility (Section D)
- 10% Reliability and Durability (Section E)
- 30% Pricing

If you remove the 30% pricing fraction, the relative weight in the "Total Technical Score" in round one becomes:
- 28.6% Security and Accuracy (Section A)
- 14.3% Offeror's Ability to Support System (Section B)
- 21.4% Election Management (Section C)
- 21.4% Ease of Use and Accessibility (Section D)
- 14.3% Reliability and Durability (Section E)

SECOND ROUND (POST-DEMO)
- 35% Total Technical Score given by the VESC in Step One
- 30% Pricing
- 17.5% Evaluation by Evaluation Committee of [mock election]
- 17.5% Evaluation by Public Voters. Mock election

ULTIMATE WEIGHT IN FINAL ROUND
- 35% Evaluation of mock election
- 30% Pricing
- 10% Security and Accuracy (35% * 28.6%)
- 7.5% Election Management (35% * 21.4%)
- 7.5% Ease of Use and Accessibility (35% * 21.4%)
- 5% Offeror's Ability to Support System (35% * 14.3%)
- 5% Reliability and Durability (35% * 14.3%)

SUBJECTIVE CLASSIFICATION STARTS:

Now, let's look at the meaning of those labels. These three probably boil down to ease of use and "featurefull-ness", when you consider how they're arrived at (one day demo for the mock election):

35 Mock Election
7.5 Election Management
7.5 Ease of Use and Accessibility

50% Total ease of use and feature-richness

So that yields:
50% Ease of use and "Features"
30% Cost
10% Security and accuracy
5% Reliability and Durability
5% Support

When one further aggregates the last items as cost elements, which is largely valid, one gets:
50% Ease of use and "Features"
40% Cost (and durability and support)
10% Security and accuracy