HART intercivic

March 30, 2007

The Honorable Debra Bowen
Secretary of State
State of California
1500 11th Street, 6th Floor
Sacramento, CA 95814

By email: votingsystems@sos.ca.gov

Dear Secretary Bowen,

Hart InterCivic is pleased to participate in the Top-to-Bottom Review of electronic voting systems being proposed by your office. We agree that the voting process should be transparent for the public, and that reasonable assurances achieved though voting systems inspection is good public policy.

We have reviewed the proposed guidelines for this undertaking, and we have three general concerns which are illustrated below in several examples. First, we are concerned that there are very little objective criteria for judging whether a voting system meets the criteria for pass or fail. Based upon the lack of specificity in the guideline, we could not confidently build a voting system with foreknowledge that it would pass or fail the California requirements. Obviously, the same concerns apply to our legacy systems.

Our second general concern is that the guidelines seem to add new conditions to continuing certification. It is likely that all voting systems presented for certification will lack some feature added as part of this review, since those requirements did not exist when the system was first certified. The implications of a failed system are dire, and by creating new conditions for certification, mass disqualifications are the most likely outcome of this review. I am not sure that is the intention of the review.

Our third general concern is that it appears that the focus of the review is on prevention under any attack scenario. This is certainly a worthy investment of time to understand threats and ways to counter them. Our system is architected with specific threats identified, and I am sure other vendor systems are as well. However, every threat cannot be anticipated, and it is unlikely that any system for voting, including paper, can be so constructed. Accordingly, we place a great deal of emphasis on detection as well as prevention - both for electronic and paper based systems. Our systems are data rich with event and audit logs, all of which can be mined for evidence of malfeasance or other failure. This is a critical part of our defense in depth strategy, and we hope that it will have strong weight in the review process.

Some of the specific examples that support our general concerns include the following:

1. You have proposed direct recording electronic (DRE) voting systems and all system media be secured against untraceable vote tampering during the

manufacture, transport, and storage of these devices. We are not certain what this means. Hart's system is currently manufactured in a secure facility, but proof of non-tampering is a hard concept to grasp. How do we prove this condition? There are secured carriers that could deliver the equipment, but the cost is considered prohibitive by our customers, and again we are faced with the prospect of proving an event did not happen. How would we set about this task? Further, these voting systems are outside of our control once delivered, so the burden of meeting these conditions falls to our customers, who will surely have the same concerns regarding compliance to these standards. All of these same concerns relate to software as well as hardware.

2. Secure testing is a laudable process, including red teaming and source code review. However, we are concerned that these tests be performed under realistic conditions in an election. Your guidelines suggest that you will provide source code to an expert and ask that person to subvert the system. It is almost certain that would be possible under these conditions. However, these are extreme circumstances, not taking into consideration real world use cases. A public pronouncement that elections software is vulnerable to attack, however, unlikely, seems to us to be counter productive to the goal of the review – increased voter confidence.

3. The source code review is a common practice and a necessary one. We have submitted to many, many reviews. However, again we are not certain what standards you will apply to this review. Your objective "to identify anything in the code that could be used maliciously" is not clear to us. What does this mean? Is it a hunt for existing failures or breaches in the code, or a subjective assessment of the software approach?

4. Disability access is of a paramount importance to us. In fact, we pioneered many of the assistive devices now used in this industry (sip and puff, unique shapes for user controls, and a form factor similar to all other voting devices used in an electronic system). However, you have added conditions for continuing certification that are incremental to existing federal standards and even the most recent State certification requirements. These new conditions will likely cause the immediate failure of most, if not all, of the legacy voting systems in California. This is especially true based upon the interpretation of item II,2.f.

There are two other concerns not specific to the guidelines themselves which, nevertheless, should be considered as potential outcomes of this review. First, it is simply not possible in today's regulated environment to respond to any new requirements in time for implementation before February, 2008. A typical process to update any code takes upwards of a year to implement, including software design and coding, internal testing, third party testing, EAC approval, and state certification processes including functional and volume testing. Manufacturing specifications and tooling (which cannot begin in production mode until we know if the voting system will be approved as proposed), actual product build and assembly, and deployment in a jurisdiction, including essential training activities, likewise will require considerable planning and time. This process implies that any changes are unlikely in 2008 under the best of circumstances.

Second, we would be remiss if we did not highlight the fiscal implications of this review to our customers. The process outlined in the preceding paragraph is extremely costly, even for minor changes. Some of the incremental conditions for certification could involve form factor changes, which can be quite expensive. For example, if text to speech readers are required, the cost can range up to $1000 per unit. Other changes to the voting system will require new firmware or even new additional circuit boards, again an expensive proposition.

When Hart InterCivic first introduced an electronic voting system to the market, our customers and prospects told us that they had limited budgets, and that our solutions simply had to become more affordable. Accordingly, we made tradeoffs. For example, variable playback speed is certainly a desirable feature, but the cost compared to the inconvenience occasioned by twice yearly use for only a matter of minutes seemed to be a practical tradeoff. Responding to market pressures, we were able to drive down price points from greater than $5,000 to less than half that amount – without sacrificing any accuracy or security. This had the overall effect of enfranchising voters with special needs. Now we sell voting systems at a price point nearing $4,000 because of added conditions for certification and manufacture. Almost anything is possible with time and money, but new requirements will again increase the cost of the compliance to our customers.

Finally, we want to make the point that voting systems are managed by our customers. We are responsible for providing first class tools, to be sure, but security is a combination of people, processes and technology. We urge your top Top-to-Bottom Review team to consider all these factors when constructing guidelines and assessing the effectiveness of security measures for all systems.

Thank you for your consideration of our response. We would be happy to discuss in greater detail any of these issues with you.

Regards,

David E. Hart Chairman

cc: Lowell Finely

[redacted]