OPEN VOTING CONSORTIUM
Alan Dechert, President
9560 Windrose Lane
Granite Bay, CA 95746 USA
Phone-916-791-0456 Fax-916-772-5360
www.openvotingconsortium.org

Monday, February 26, 2007

Mr. John Arntz
Director, Department of Elections
City & County of San Francisco
1 Dr. Carlton B. Goodlett Place
Rm 48
San Francisco, CA 94102

> ***We are going to eliminate private, invisible, proprietary software that no one can evaluate as a means of counting our votes.***
> — California Secretary of State Debra Bowen, Inaugural Address, January 2007

Dear Mr. Arntz,

I am writing in response to your February 20th memo (Memo)[1] to members of the San Francisco Board of Supervisors.

I appreciate very much the fact that this Memo is freely available on the Internet for anyone to scrutinize. San Francisco has shown an extraordinary commitment to transparency in government, and has been a leader in the promotion and adoption of sunshine laws. Government is the business of The People. We all agree that there is no place for secret maneuvering among government officials. The People have an absolute right to know what their government is doing and planning to do.

We also agree that elections are public processes, and that there is no place for secret procedures anywhere in the voting system. Open Voting Consortium (OVC) promotes complete transparency in election administration. This is the Open Voting idea. We support candidates that embrace this idea — opposing and seeking to educate or remove officials that do not. We sponsor and/or promote legislation that is consistent with Open Voting. We also promote standardization and transparency in voting system technology, and we assist with engineering expertise.

Last year, OVC sponsored AB 2097[2] (Goldberg), which was co-authored by San Francisco Assembly Member Mark Leno. This bill would have required disclosure of voting technology in a way similar to what we are now seeking in San Francisco. We have revised the bill in such a way that we are confident it will pass this year.

[1] See http://www.ci.sf.ca.us/site/uploadedfiles/election/Elections_Pages/20070220.pdf

[2] See http://www.leginfo.ca.gov/pub/05-06/bill/asm/ab_2051-2100/ab_2097_bill_20060504_amended_asm.html

It is now AB 852 [3], carried by Assembly Member Paul Krekorian of Los Angeles. If we are right about the chances, this will be in the body of California law: *"All details of election administration must be made freely available to the entire public in a regular and systematic way."* This includes all details in the voting system technology, including source codes.

Former Secretary of State Bruce McPherson feigned support[4] for OVC initiatives. In fact, he stood in opposition to us. We are very wary of similar behavior patterns we sometimes see in government officials. He sandbagged the report called for by Assembly Concurrent Resolution 242 [5] (Goldberg), passed by the Legislature in 2004, sponsored by OVC. Then he vigorously opposed[6] AB 2097. Fortunately, McPherson is no longer Secretary of State.

I am sure you also agree that when the government spends money, it's spending money that still belongs to The People. We, The People, have an absolute right to approve or disapprove of any expenditure of our money. I'm not a San Francisco resident, but when you are talking about spending state and federal "grant" money, you are talking about spending money that also belongs to me.

I do not want my money spent on secret proprietary technology. If we're going to spend public money on technology, it should be public technology. I believe this principle should apply to government procurement everywhere. Security by Obscurity is a failed computer security model. It just doesn't work. It only serves to facilitate vendor lock-in. The last place in the world that proprietary technology should be tolerated is the voting system. If we want to know exactly how the technology works, we can demand that before we spend the money.

You have invited OVC for dialog, and we appreciate that. This is a good sign. However, your Memo is disturbing for several reasons. OVC is concerned and dismayed by the fact that you are vigorously pursuing a contract for voting systems that include private, invisible, proprietary software when the Secretary of State has declared that she intends to eliminate these secret procedures.

[3] See http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_0851-0900/ab_852_bill_20070222_introduced.html

[4] See http://www.openvotingconsortium.org/ad/sos-letter-921.pdf

[5] See http://www.leginfo.ca.gov/pub/03-04/bill/asm/ab_0201-0250/acr_242_bill_20040831_chaptered.html

[6] See his letter in opposition http://www.openvotingconsortium.org/ad/sos-opposition-letter524.pdf and my response http://www.openvotingconsortium.org/ad/OVC2SOS-525.pdf

On January 19th, you issued a press release[7] announcing that you will establish "an open source voting system task force." We applauded you then, and we are still hopeful that you will follow through with this. Your Memo includes an appropriate definition of "open source." However, your actions make me wonder:

- Were you using the same definition of *open source* when you wrote the January 19th press release?
- Could this task force be described as pro-*open source* or anti-*open source*?
- Has the task force been formed, and if so, what has been done so far?

I'm sure that your announcement about this task force was not a smoke screen like we've seen from McPherson and others. The reason for my questions is that you are now arguing strenuously to protect the vendor's intellectual property rights.

Steven Bennett was quoted in Thursday's paper[8] saying that Sequoia would not disclose because it would "jeopardize the security to all of our customers in California and across the country."

Apparently, Sequoia fears sunshine a killer, not a disinfectant.

They appear to be admitting that there are security vulnerabilities in their technology. However, suppressing public scrutiny cannot ensure that the vulnerabilities will be inaccessible: if the vulnerabilities are there, hiding them will not make them go away. Who knows how many people have Sequoia's source code now? Former employees, former owners, former test labs … who knows if they're all trustworthy? Besides, you don't necessarily need the source code to find the vulnerabilities[9].

These security vulnerabilities are like land mines. If you were traveling through a field known to have land mines, would you be safer knowing where the land mines are, or not knowing? You are going to be better off if the land mines are identified and flagged. That way, you can work around them and defuse them when you have the resources to do so.

Open is more secure. In the Assembly Elections Committee hearing on AB 2097 last April, San Francisco resident and open source software expert Josh Berkus[10] was one of our star witnesses.

[7] See http://www.sfgov.org/site/election_page.asp?id=53715

[8] See http://gnosis.python-hosting.com/voting-project/February.2007/0131.html

[9] See http://www.votelaw.com/blog/archives/election_administration/voting_machines/

[10] See http://www.openvotingconsortium.org/ad/openvotinglobby.pdf
for more on the APR 18 hearing, see http://www.openvotingconsortium.org/blog/2006-apr-26/no_opposition

Mr. Berkus has been on the Core Team that produced PostgreSQL (Open Source database software with over 15 million users). This database software has been cited as the most secure database system in existence.

We were anticipating that three of the seven committee votes would go against us. We won the vote five to zero. Two Republicans that started out opposed to the bill abstained. The security by obscurity issue was one of the main topics.

Sequoia's intellectual property has no commercial value to anyone other than Sequoia. Why do you seem so interested in protecting it? Indeed, it may have little value even to Sequoia. Once Secretary Bowen’s transparency imperative is in force, how will Sequoia sell technology they’ve publicly proclaimed non-secure if disclosed?

The security of Sequoia’s voting systems would be no more easily compromised if disclosed, anymore than Diebold’s was when their code was accidentally released on the Internet. It was embarrassing to Diebold for the world to find such ridiculous security measures as a hard-coded password of “1111” for administrator access. The public doesn’t have physical access to the machines in order to enter the password.

If Sequoia representatives show up at another board meeting, I would like to see some follow up questions about why they don’t want their code disclosed. Does their code include things that would embarrass Sequoia in front of the engineering community? Is all their technology properly licensed, or do they fear legal exposure for using technology that is not quite kosher for them to use?

There are two ways to approach development of voting technology: the standard way, and the non-standard way. The standard way is the correct path. Any other way is simply wrong. Innovative vote counting methods are not necessary, not desirable, and should not be accepted. The technology is relatively simple and well understood. Vendors only prefer their proprietary methods as a way to carve out market niches.

OVC promotes open and *standard* methods, such as the OASIS Election Markup Language[11] (EML). OVC project members participate in various standards bodies including IEEE as well as the OASIS Election & Voter Service Technical Committee. The OASIS EML is an international standard that covers nearly all the voting system requirements for the United States as well. We are working with

[11] See The Case for using Election Markup Language (EML) http://www.oasis-open.org/committees/download.php/22101/The%20Case%20for%20EML.pdf
Notice Appendix C, Case Study #5 “Open Voting”

OASIS and the National Institute of Standards and Technology (NIST) to ensure that the EML will handle all the requirements in the U.S.

John Borras, chair of the OASIS Technical Committee for the EML, recently wrote to me with the following comments about what we need for an e-voting standard. I agree with this, and OVC will be adding more specifics over time.

> *An open[12] public e-voting standard must:*
>
> - *Have open public license terms that are free for use and that permit open source implementations*
> - *Be publicly available, documented and accessible via the Internet*
> - *Ideally be a de jure[13] standard*
> - *Have a controlling body that should be open with available public membership, with open public processes, archives and access to the specifications development process*
> - *Be controlled by an open approval process that has a well-defined, inclusive process, with public comments and input for evolution of the standard*
> - *Have approval of the standard that is subject to review and voting across the membership of the defining standard organization*
> - *Support the provisions enshrined in a Voter's Bill of Rights or other similar legislation*
> - *Be broadly implementable by available e-Voting systems and not be designed to be restricted to only a few providers' solutions*
> - *Be adaptable by design so that localization and extensions are permitted, supported and anticipated*
> - *Produce consistent results that can be independently verified by anyone familiar with the standard and specification details*
> - *Be auditable for conformance, compatibility and support the development of verification testing tools*
> - *Support interoperability amongst vendors' implementations so that parts of the e-voting process can be separately and independently developed and then interact successfully*
>
> *Using such an open standard will help, along with associated traditional administrative and manual election processes, secure a result that is trustworthy, verifiable and affordable.*

The coming nonproprietary election technology also implies a different business model: the *service* model. Vendors will not make money on the technology, but on services that surround the use of that technology. This model is working well for companies doing business now with open source software in other fields.

[12] Open = Approved under an open process where all interested parties have input, results are publicly viewable, etc. The organization who developed the standard may be de jure or not.

[13] De Jure = Force of law; approved by one of the four recognized international standards organizations (ISO, IEC, ITU, UN/ECE)

Apache web server software now commands a sixty percent market share. San Francisco resident, Brian Behlendorf founded Apache. Brian attended the February 21st Budget and Finance Committee meeting. He is interested in these issues, and you may remember an email[14] he sent to you a few weeks ago.

Another factual error in your Memo needs to be addressed. The last section of your memo includes "ALTERNATIVE LANGUAGE PROPOSED BY 'COUNT AS CAST'." The language given here was proposed *in addition* to the disclosure language, not as an alternative. There is no such "Count As Cast" group to my knowledge. Jim Soper has a web site at www.countedascast.com but he has no such group, and does not contemplate organizing one. I believe he is addressing your mistake in a separate email to you and the Board.

Please don't mischaracterize what OVC is proposing! You state that we go "beyond opening the source code of voting systems." The contract language we provided is for disclosure only. The contract language, strictly speaking, does not require open source (disclosed source under "relaxed or non-existent intellectual property restrictions" as you say. See AB 852 or the Open Source Initiative for a more precise defintion). The vendor would still retain ownership of the technology. We want to know the hardware specifications because there is software in the hardware! We are not asking for source code for commodity-off-the-shelf components (COTS). These are things that are needed for federal certification, so your vendor should have no problem supplying these things. Note that under federal certification guidelines, customized components are required to be reviewed. COTS components do not need to be reviewed, but they need to be identified. That's all we're asking.

This part of your Memo is especially remarkable:

> ***Sequoia will not agree to this language due to business concerns that their system would be replicated. Sequoia's concerns do not seem unfounded—the President of OVC, Alan Dechert, recently stated during public comment that the OVC is participating in the building of voting systems expected to reach the marketplace by 2008.***

I know that you don't mean to say I want to steal Sequoia's technology. You surely understand that I have no interest in Sequoia's technology other than disclosing it in favor of the transparency imperative.

OVC has demonstrated open source technology, but not for a DRE. Sequoia is providing DRE (Direct Record Electronic) technology. OVC is opposed to DREs and favors systems where the paper ballot is the fundamental representation of the vote. With a DRE, we don't even know what constitutes a "ballot."

[14] See http://www.openvotingconsortium.org/ad/brian1-22.pdf

The law that established the paper trail for DREs says that the *paper record copy* of the vote *is not a ballot*! Instead, OVC has demonstrated Electronic Ballot Printer technology where the voter makes selections on a computerized system, and the ballot is printed out on the spot. Our April 2004 demo at the Santa Clara County government center was lauded coast-to-coast[15]. The United States Government Accountability Office (GAO) also cited us as a key non-governmental initiative aimed at improving voting system security and reliability[16].

We work with Open Voting Solutions, Inc. (OVS), a for-profit corporation established in New York and Maryland. We have no financial interest in OVS! OVS has also demonstrated an Electronic Ballot Printer, as well as an optical scan system that utilizes off-the-shelf scanners and other off-the-shelf components.

The OVS optical scan system is nearly ready for commercial application. We need a way to fund certification. The engineering work has been collaboratively done. It's free software.

You have this part backwards. Disclosed technology (as we propose in the contract language, not open source) does not enable stealing. It would actually make it harder to steal since any technology stealing would be easier to spot with disclosed systems.

Obviously, we are not interested in using Sequoia's technology. Disclosing it does not enable legal use by others, and the technology we have developed has nothing to do with Sequoia's technology. You may, however, want to clarify what you do mean when you imply I want it because I'm helping with making a system commercially available by 2008. It sounds like nonsense to me, but perhaps you can help us to make sense out of it.

I am glad to see you state, *"I am committed to transparency and am very willing to work with the Board to increase transparency in San Francisco's voting system and to move toward an open source voting system."* But then you say, "Combining the concepts of Sequoia's proposed language with Mr. Soper's provides an effective solution…." I don't think anyone believes that, including Mr. Soper.

[15] See Mercury News Editorial, *The Touch Screen Holy Grail*
http://www.openvotingconsortium.org/ad/sjmerc0408.pdf
and Baltimore Sun, http://www.dalelane.co.uk/cache/ovc_news4.htm

[16] See http://www.openvotingconsortium.org/ad/gao-p51.pdf

Sequoia is simply saying that it will comply with any changes in election law that may be coming. We already know you and Sequoia will comply with the law. We are asking you to take a leadership role for transparency in election administration, instead of sinking millions of dollars into obsolete technology, business as usual.

If you are really interested in facilitating an open source voting solution, you should get started immediately with the RFP process specifying ***open source***. You mentioned that you don't have the staff to do another RFP right now. I am recommending to the Board of Supervisors that they find the resources to get this RFP process started immediately. I am also asking the Board to formally adopt a policy requiring technology disclosure for voting technology.

We look forward to talking with you soon to discuss ways our team can assist your office in meeting your objectives.

Please call me at 916-772-5360 or email me at alan@OpenVoting.org.

Sincerely,

Alan Dechert

Cc: Members, San Francisco Board of Supervisors
Members, San Francisco Elections Commission
Dennis Herrera, City Attorney
Ed Harrington, Controller
Phil Ginsburg, Mayor's Chief of Staff
Ann O'Leary, Deputy City Attorney
Steven Bennett, Sequoia
Howard Cramer, Sequoia
Lowell Finley, Deputy Secretary of State
California Assemblymember Paul Krekorian
California Assemblymember Mark Leno
California State Senator Leyland Yee, Ph.D., Assistant President pro Tempore
Various citizens, groups, and members of the media interested in having transparent elections