Alan Dechert's Testimony in favor of AB 2097, April 18, 2006

Secretary McPherson's assertion (April 17, 2006 letter):

> *Allowing unqualified, non-expert access to source code and providing detailed instructions for building voting systems software, could compromise the system security and result in the manipulation of elections.*

This assertion is absolutely false. In fact, the opposite is true. Open systems are more secure. You can't achieve system security by hiding vulnerabilities. "Security by obscurity" has proven not to work. Hackers can find vulnerabilities without this documentation.

Publication of these details will make voting systems **more secure** in the short run and in the long run.

1) Long run: Exposed vulnerabilities will be seen by a large audience of scientists and engineers. These problems can be discussed and then corrected.

2) Short run: These vulnerabilities are like landmines. If you were walking across a field known to have landmines, would you prefer not to know where they are located? Better to have them flagged so we can work around them and defuse them.

Election problems in 2000 and 2004: We have studied this issue as a nation and the State of California

1) US General Accountability Office (GAO-05-965 Electronic Voting Systems)
http://www.gao.gov/new.items/d05956.pdf
> *pg 51 cites Open Voting Consortium as a "key initiative" for making the voting system more secure and reliable.*

2) ACCURATE, National Science Foundation Center
http://www.accurate-voting.org/accurate/docs/2005_vvsg_comment.pdf
> *III. TRANSPARENCY AND PUBLIC OVERSIGHT*
> *The process for establishing voting technology must be reformed to provide transparency. Transparency is the extent to which the process and technology used in elections is open for inspection by members of the public, no matter what their situation or background.*

3) CA Secretary of State report on open source
http://www.ss.ca.gov/elections/open_source_report.pdf
> Lawyer and Carnegie Mellon computer scientist, voting machine examiner for 20 years in PA, Dr. Michael Ian Shamos quoted: *"all voting system software should be disclosed to the public."*

4) CA State Senate Hearings on open source
Bowen announces dates on "Open Source Voting" concept and how voting equipment is certified
California Chronicle , Jan 28, 2006
> *"If we want people to have confidence that their votes are being counted accurately, the process we use to certify machines for use in this state and the systems themselves need to be open, accessible, and completely transparent…."*

5) SoS's Voting Systems Technology Assessment Advisory Board, *Security Analysis of the Diebold AccuBasic Interpreter*
http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf
Egregious security fault found in Diebold tabulator. Diebold repeatedly denied it. Vendors conspired to black list Leon County FL elections chief. On Feb 27, Diebold Corporate General Counsel told Leon County Board of Commissioners they would never sell systems to Leon County as long as Sancho was in charge. This report vindicated Sancho. When vendors say, "trust us," should we?

These reports all point to the same idea: open up the system; get rid of the secret processes.