



"Riveting"
— *Vanity Fair*
"The gospel of the
movement"
— *Time Magazine*



6/16/05: Request to the California Secretary of State Under Election Code 19202

Jim March, Member of Board of Directors, Black Box Voting 916-370-0347 / jmarch@prodigy.net
Bev Harris, Executive Director, Black Box Voting 206-335-7747 / bev@blackboxvoting.org

EC19202 reads as follows:

Any person or corporation owning or being interested in any voting system or part of a voting system may apply to the Secretary of State to examine it and report on its accuracy and efficiency to fulfill its purpose. The Secretary of State shall complete his or her examination without undue delay.

Black Box Voting, Inc., a nonpartisan, nonprofit, 501c(3) consumer protection organization for elections, requests a formal examination under this statute of a specific Diebold Election Systems component: the programmed "electronic ballot box" memory cards used in optical scan and touch-screen voting systems.

As your office may be aware by now, Black Box Voting, Inc. was allowed to test the Leon County, Florida Diebold optical scan system (firmware 1.94w). During this testing, we proved that Diebold memory cards contain executable code, that the firmware in the optical scan places a "call" to the executable code on the memory card, and that the operation of the election system can be changed in various malicious ways without detection. We succeeded in loading altered code onto the optical scan via the memory card, which altered votes undetectably. We also succeeded in pre-stuffing the ballot box in a way that does not alter the overall number of votes, but flips a predetermined number of votes to another candidate.

We specifically request that the Secretary of State's office evaluate the following:

1. Whether or not executable code is present on these cards;
2. Whether or not the firmware of the touch-screen and/or the optical scan (either precinct count or central count) ever places a call to executable code on the memory card;
3. Under what specific conditions any executable code on the memory card is checked by the firmware for accuracy (via checksums, hashes, file size);
4. Whether or not it is possible to load manipulated code on the memory card so as to perform malicious functions such as vote shaving, vote "skimming," vote changing, altered reports, altered audit log, pre-stuffing of the ballot box, over-writing results of other precincts, or any other substituted code;
5. Whether or not it is possible to override and invalidate the California certified version of the firmware or software by executing program "updates" via the memory card.

We make this request for:

1. The latest optical scan systems (firmware 1.96.4);
2. The paperless touch-screens as used in Alameda County on Nov. 2, 2004;
3. The new TSx system proposed for certification;
4. Any older optical scan models still in use in California.

Note that on touch-screen precinct terminals, the exact filenames involved on the memory card and the type of executable may be different than those on the optical scan systems. The call to the executable may be obscured in Dynamic Link Library (".dll") files. We have found references to this under the name "abc." All files under the name "abc," AboBasic," "AccuBasic," and "ABasic" should be examined to determine exactly where they are invoked in system designs for all Diebold voting equipment.

We also have evidence that altered code can be centrally loaded on ALL cards from GEMS by altering files at the **C:\PROGRAM FILES\GEMS\ABASIC** directory, propagating the "hack" either county-wide or to hand-selected precincts as a batch. We believe the altered code can be linked to a specific day, can be loaded months or even years prior to elections, and can be constructed so as not to appear during pre-election and post-election Logic and Accuracy tests.

Both of us have personally witnessed Diebold employees, other contractors, and even local volunteers handling Diebold memory cards, unsupervised by county officials.

We are convinced that a design which invokes executable code on a memory card is unsupportable in a certified software environment where security is of critical importance. This code is allegedly "certified," but if a standard feature exists within the design allowing alteration of code on removable modules, long after certification and even during the middle of elections, the intent appears to be to provide a vote-tampering mechanism. This Diebold design clearly sacrifices security for "flexibility" – and in the election environment, that translates to "quick and easy tampering."

We ask for a timely response on this matter. Regardless of what you find, we request that a formal report be issued to address these issues as soon as possible.

Jim March
Member of the Board of Directors
Black Box Voting, Inc.

Bev Harris
Executive Director
Black Box Voting, Inc.