

NO DEAL WITH DIEBOLD!

PROBLEM: DIEBOLD IS AN IRRESPONSIBLE BUSINESS PARTNER

• From the office of California Secretary of State; *STAFF REPORT ON THE INVESTIGATION OF DIEBOLD ELECTIONS, INC*¹, April 20, 2004: "In sum, Diebold:

1. marketed and sold the TSx system **before it was fully functional**, and **before it was federally qualified**;
2. **misrepresented** the status of the TSx system **in federal testing** in order to obtain state certification;
3. **failed to obtain federal qualification** of the TSx system despite assurances that it would;
4. **failed even to pursue testing** of the firmware installed on its TSx machines in California until only weeks before the election, choosing instead to pursue testing of newer firmware that was even further behind in the ITA testing process and that, in some cases, required the use of other software that also was not approved in California;
5. **installed uncertified software** on election machines in 17 counties [including Humboldt²];
6. sought last-minute certification of allegedly essential hardware, software and firmware that had **not completed federal testing**; and
7. in doing so, jeopardized the conduct of the March Primary."³

PROBLEM: QUESTIONABLE PERSONNEL

- "I am **committed to helping Ohio deliver its electoral votes** to the president next year." - Wally O'Dell, CEO, Diebold, 2003 (The New York Times, 9 November 2003; "Machine Politics In the Digital Age"). The Diebold CEO also organized a \$600,000 fund-raising party for the Mr. Cheney (Akron Beacon Journal, 1 July 2003).
- Jeffrey Dean has **23 convictions for computer-embezzlement**. In 2000 Dean became head of research and development at Global, and worked on the voting and tabulation machines. He also became a director of Global that same year. As Diebold was buying Global, Dean left the company, but Diebold hired him back as a consultant.⁴
- Diebold and rival Election Systems and Software are run by brothers Bob and Todd Urosevich, respectively. The two companies count approximately 80% of the votes in the U.S.⁵

PROBLEM: VOTER CONFIDENCE CANNOT BE ASSURED

- A mission-critical system that actually counts votes must be tamper-proof. Diebold's GEMS **vote tabulation** program is **wide open to election fraud**.

"Right now you can open GEMS' .mdb file with MS-Access, and alter its contents. That includes the audit log. ... Jane ... did some fancy footwork on the .mdb file in Gaston recently. I know our dealers do it. King County is famous for it. That's why we've never put a password on the file before."

— Ken Clark, Principle Engineer at Diebold, email, 18 Oct 2001^{6 7}

The use of MS Access — well known as **not secure** — to count votes is appallingly **unprofessional** for a mission-critical product — lacking mandatory password protection is worse.

- In their study of 2002 Diebold computer source code, four computer security experts "conclude that this voting system is **unsuitable for use in a general election**." They go on to say "Our analysis shows that this voting system is **far below even the most minimal security standards** applicable in other contexts."⁸
- Diebold machines have a long history of **miscounting votes**.⁹

In summary, Diebold wants our business. But it is not clear they care how they get it or what they will do once they get it. Diebold shows little regard for the integrity of the voting system and leaves no basis for confidence in the results they produce.

WHAT WOULD BE BETTER? – FLIP THE PAGE TO LEARN ABOUT OPEN VOTING CONSORTIUM

1 Diebold bought Global Election Systems in January 31, 2002.

2 http://www.ss.ca.gov/elections/ks_dre_papers/randgsummary.pdf

3 http://www.ss.ca.gov/elections/ks_dre_papers/diebold_report_april20_final.pdf

4 http://www.blackboxvoting.org/bbv_chapter-8.pdf, pg. 84

5 <http://www.ecotalk.org/UrosevichBrothers.htm>

6 <http://www.equalccw.com/smokinggun.pdf>

7 <http://www.scoop.co.nz/stories/HL0307/S00065.htm> "Inside A U.S. Election Vote Counting Program"

8 <http://www.avirubin.com/vote.pdf> "Analysis of an Electronic Voting System", T. Kohno et al

9 <http://www.votersunite.org/info/Dieboldinthenews.pdf>

SOLUTION: OPEN VOTING CONSORTIUM

More and more, citizens are expressing dissatisfaction with a voting system that is largely privatized and systematically excludes people from participating in the most basic process of any democracy. In short, the answer to closed voting is open voting.

As the [San Jose Mercury News](#) pointed out over a year ago, "The government unwisely ceded development of electronic voting machinery to private companies like Diebold Voting Systems, whose proprietary software is under electronic lock and key. The secrecy of the source code, a slew of malfunctions, and a lack of a paper copy that voters can look at have eroded confidence in touch-screen voting."¹⁰

Open Voting Consortium (OVC) seeks to **restore the ability of the people to be involved** in one of the most basic activities in any democracy: counting the votes. As Mike Himowitz of the [Baltimore Sun](#) put it, "Critics also complained that these systems use proprietary software from their vendors to tabulate and store votes -- code that's not available to the public. In essence, the most critical part of the election -- counting the votes -- had been snatched from public view and stashed away in a 'black box.'"

Traditional software companies hate **open-source software** because no one owns it or collects royalties for it. But the process works. The Linux operating system, now used on millions of servers around the world, is a premier example of open source software. Computer experts say Linux is **far more secure** than Microsoft Windows -- largely because friendly hackers have examined it closely and suggested improvements that help keep intruders out."¹¹

OVC has developed prototypes of publicly programmed voting and vote-counting machines. The voting machines **print** the actual **paper ballot** that is used for counting. They also write a permanent record of the ballots to CD-ROM. This **prevents ballot box stuffing** and "lost" ballots. The prototypes demonstrate a design that will **protect the rights of the disabled** to vote without assistance, and support all scoring methods in use such as instant runoff voting.

OVC is seeking funding to turn these prototypes into tested, certified voting systems. These voting systems will be secure, reliable, and open to inspection. The **software** will be **free**, and the **hardware** will use **inexpensive**, off-the-shelf parts. See the Ballot Reconciliation Procedure Guide¹² for the step-by-step path taken by each vote from the voting booth through counting and archiving for potential re-counting. For further information, and to support clean elections, please visit www.OpenVoting.org.

Open Voting Consortium can **reduce costs** and **increase public confidence** in the voting system. Standardized, open, public software will attract many engineers in the open source community to assist in software development and testing. The open source development and maintenance model has proven successful with some of the most widely used programs on the Internet.

If you want to have the option of an open voting system available for counties in your state, let your Secretary of State and State Assembly know today. Help America Vote Act of 2002 (HAVA) funds should be available to support research and development of open voting systems. The Open Voting Consortium works with public universities to research and develop open voting systems. Why not have public money be made available for public universities to develop a public voting system for your state?

To arrange a FREE DEMO of the OVC voting system, please contact Lara Shaffer at 831-419-0758.

¹⁰ <http://www.kentucky.com/mld/mercurynews/news/opinion/8383100.htm>

¹¹ http://www.dalelane.co.uk/cache/ovc_news4.htm

¹² <http://www.openvotingconsortium.org/ad/brp-guide.pdf>