

Nationwide electronic voting problems have occurred in Humboldt

--**Modem failures** (precincts could not transmit results to election HQ): 27 failed in March 2000, four in June 2006 and 16 in Nov. 2006. CA banned modems in Aug. 2007.

--**Memory card failures** (the “electronic ballot box” within the Diebold optical scanner) occurred in 2000, including one precinct that failed twice; Eureka and Arcata also experienced memory card failures in June 2006.

--**Full machine failures** resulted in Diebold optical scanners being replaced during Election Day, November 2006, in Arcata, Blue Lake, Eureka, and Fortuna.

Who is Diebold?

--Diebold is the company that makes our voting machines and controls the secret software inside them. Diebold recently changed its name to Premier.

--Diebold admitted breaking the law in 2003 by installing uncertified software in voting machines in Humboldt and 16 other CA counties. No action was taken against Diebold.

--Prior to the 2004 election, Diebold’s then-CEO Walden O’Dell wrote a fundraising newsletter pledging to “deliver Ohio’s electoral votes to the President.”

-- In December 2005, Diebold shareholders filed multiple class-action lawsuits alleging securities fraud and that Diebold was “unable to assure the quality and working order of its voting machine products.”

Just how bad is their equipment?

--In Aug. 2004, on CNBC, Bev Harris showed Howard Dean how to hack Diebold’s GEMS Central Tabulator in 90 seconds and change election results without leaving a trace of evidence.

--In Sept. 2004, The Department of Homeland Security’s Computer Emergency Readiness Team listed Diebold’s GEMS Central Tabulator *as a threat to national security*. (In 2007, Humboldt still uses GEMS to add up precinct results).

-- Diebold’s optical scanners use “interpreter code” to scramble vote choices from a ballot into AccuBasic, the *trade-secret* proprietary language of Diebold. That means the vote is counted in secret and neither the public, nor the media, nor even the elections department can verify the accuracy of the results without a 100% hand count.

--Reports by computer security experts have detailed flaws in the design of Diebold’s optical scanners. California’s recent Top To Bottom Review of electronic voting machines concluded that no “procedural mitigations” could make the machines completely secure, and yet the flawed and hackable machines remain in use.

Is this what passes for security?

--Because anyone with even brief access to a memory card can undetectably alter election results, voting machines are supposed to be accompanied by two or more people at all times, yet are sent home with pollworkers (“Sleepovers”) for days prior to Election Day.

--Tampering with memory cards can change election results, with or without direct access to the memory cards, and whether or not the card is “sealed” in the machine.

We appreciate donations to offset costs

Voter Confidence Committee • PO Box 5131 • Eureka, CA 95502
www.VoterConfidenceCommittee.org