

PUBLIC RECORD ACT REQUEST

Responding Agency: Alameda County Registrar of Voters
1225 Fallon Street G-1, Oakland, CA 94612-4283

*A second copy of this PRAR will be presented to the
Alameda County Board of Supervisors as an advisory notice.*

Date filed: 7/29/03 by Jim March / Email: jmarch@prodigy.net / fax: 707-221-7152

Please note: all URLs (anything starting with "http://") are case sensitive in any Internet browser.

Introduction (reason for filing PRAR):

Concerns about electronic voting systems (especially systems that leave no physical paper trail) have been common for some time. Also of concern is the typically proprietary nature of the software, with the source code held private as a "trade secret" – no independent security analysis can normally be performed.

These issues are currently being reviewed by the California Secretary of State's office.

In January of 2003, activists concerned with these issues were exploring the website for a major vendor of electronic voting systems. They found an "FTP" (File Transfer Protocol) area devoted to exchanging company files, including test data, compiled program code and source code. The FTP site was set up for "anonymous access with no passwords" so it can hardly be described as a "hacker break-in".

The company involved was Diebold Election Systems, for their "Accuvote-TS" product. This product, by this vendor, is in use by the county of Alameda.

As of July of 2003, two different groups have analyzed the security "features" of the product. So far, the one that has gotten all the attention has been the one performed by John Hopkins University (see also: <http://avirubin.com/vote.pdf> dated July 23rd). Running 24 pages, it is scholarly in nature and analyzes the software running on the touch-screen workstations where the actual vote takes place. Significant flaws were identified, but Diebold's response has some merit (<http://www.diebold.com/statement.htm> and <http://www.diebold.com/technical.htm> both dated July 25th). In summary, Diebold explains that the vote-stations are not connected to the Internet and hence with proper physical access controls (reasonable care at the polling place) security is adequate. The John Hopkins study has received some media attention, notably <http://www.signonsandiego.com/news/computing/20030724-1328-electronicvotingflaws.html> and http://www.onlineathens.com/stories/072503/new_20030725026.shtml among others.

However, the John Hopkins study wasn't alone. A different analysis was done by a group of "techies/activists" led by Bev Harris (also known as "the Scoop report" for where it first appeared – I will refer to it as the Bev Harris report). While not as formal in nature and layout, the allegations raised are far more serious than what John Hopkins saw. The Bev Harris report may be viewed at:

<http://www.scoop.co.nz/mason/stories/HL0307/S00065.htm> and a follow-up at:

<http://www.scoop.co.nz/mason/stories/HL0307/S00078.htm>

Harris and company analyzed the software and sample data files that would be held at the “central data collection PC” at the offices of whoever manages an election at the county level. This would be a personal computer of more conventional design than the polling-place terminals, probably an ordinary off-the-shelf system, perhaps with a card reader attached.

Harris and company found “features” that appear to not only allow for, but also deliberately *facilitate* elections fraud.

The three most damning allegations can be summarized as:

- a) General bad security – audit trails don’t work or are easily subverted, the data is stored in MS-Access, which is known for pathetic security management features, and more.
- b) The data at this central facility PC was internally stored in *three* redundant data structures. Harris & co. never established what the third one was for, but in the case of the first two, the results were horrifying: precinct-by-precinct data was pulled from the first table, while countywide tallies were pulled from the second. And there are no internal checks to make sure they match. The result? Anybody could tamper with the second data structure by adding the same number of votes from one candidate as were illicitly removed from another. So long as the total vote count remained the same, no “alarms” would be raised. And if the county-level administrators tried to do an audit of any one precinct, those numbers would come from the undoctored table #1. Only by printing out the tallies from each individual precinct and then adding the results with a hand calculator or something could you catch discrepancies between the contents of table #1 and #2. There is nothing in the software to TELL the operators that the data is stored twice and being retrieved from different data sources for different purposes. *In accounting terms, there are “two sets of books kept”*, which any accounting professional will tell you is not only “bad practice”, it’s a hallmark of fraud.
- c) The code includes a utility to “manage” (read: doctor at will) the dates of all the datafiles at once. There is no valid excuse for such a thing being there. Using it, one could alter election returns hours after the polls closed and the data from the field was supposedly inputted, and then tweak the date/time back to avoid leaving evidence.

Both the Bev Harris and John Hopkins studies were done based on the code downloaded from Diebold’s FTP site in January ’03. Diebold claims that this code is not in the field, and never was.

Methinks we better check. Fast.

The purpose of this PRAR is to evaluate the logistics of doing an on-site inspection of the Diebold software and data handling at the County Registrar’s office. The author of this PRAR fully understands that for copyright reasons, the Diebold code may not be removed from the premises, AND it’s critical that no new software or security flaws be added to the existing situation.

The questions are therefore phrased to set up an inspection in as safe and convenient a fashion as practical.

PRAR Questions:

- 1) Please list the physical locations of all computers used to centrally collect and manage polling data.
- 2) Please list the names and business contact information (preferably with Email addresses) of the county employees tasked with managing the computer(s) in query #1.
- 3) Please list an inventory of which Diebold Elections Systems programs (on CD, floppy or other media) are held at county offices. In particular, please list the title of any Diebold CD, floppy set or similar and where known, the publication date. *Whatever you do, don't throw any away, even if it is "outdated".*
- 4) Please list a contact person (preferably with Email address) of a person within the Registrar's office who will be managing the onsite inspection of the computers and Diebold CDs. It is also recommended that the Alameda County Sheriff's Office "high-tech crimes unit" or similar be informed of this PRAR and brought into the process, including monitoring the on-site inspection.
- 5) Please identify a person within the Registrar's office who can be present during the inspection and who knows how to operate the Diebold systems and software. This can be the same person as in query #4, or another.
- 6) Please state whether or not the Registrar's office has available standard commercial copies of the "Microsoft Access" database program on a factory CD. It is often included in "MS Office Professional", so that would do too. IF the Registrar's office doesn't have one, please determine if a copy can be borrowed from a trusted source within the county government, such as the Alameda County Sheriff's office. *We need to examine actual vote data, or at least the test data supplied by Diebold, to try and "duplicate the Bev Harris findings" of "doubled books", a "date diddler utility" and similar. The easiest way to do that is to load MS-Access on the same PC as the Diebold software or a set of old actual vote data to look for the "double (triple?) set of books" problem.*

It is my fervent hope that the county will fully cooperate with this analysis of "actual installed Diebold product" by the public. So far as I'm aware, such an analysis has not been done. If the Bev Harris study is even partially accurate, and deliberate "features" designed to facilitate fraud are encountered, Alameda County will have the makings of a civil suit against Diebold, and criminal charges could in theory stem from this. Which is why I'd like to see a detective familiar with high-tech crimes from the sheriff's office be brought in.

Please note: while I am a political activist in another area of concern, this matter isn't linked to any other political activity I am or have been involved in.

I would like all communication on this matter to be handled electronically (fax or Email).

Jim March - 7/29/03 - Email: jmarch@prodigy.net / fax: 707-221-7152