

Jim March / xxxx xx xxxx / Sacramento, CA 95814 / 916-370-0347

Email: jmarch@prodigy.net / Website (on elections): <http://www.equalccw.com/voteprar.html>

June 16, 2004

Ms. Goldberg,

Thank you for your sponsorship of ACR 242 (open source on electronic voting).

My purpose in writing is to provide some additional background on the subject as it affects the larger universe of personal computer software and “business politics”, and hence the opposition by “general computer industry groups” only loosely (if at all) affiliated with the actual electronic voting companies (Diebold, Sequoia, ES&S, etc.).

What you’re seeing in opposition to ACR 242 is a piece in a larger war: Microsoft versus the “Linux world”. “Linux” and its derivatives/variants are open-source alternatives to Microsoft’s “Windows” operating system. On any computer, the operating system is the “master software” that everything else “runs under”...applications must be written to a specific OS. Windows currently dominates the market; Linux is the ONLY alternative available if you have a standard Intel-based personal computer. (The Macintosh and its OS is another alternative, but for different hardware.) While capable of general personal computer use (although without as much of an established software base), Linux is gaining particular attention for it’s high security and lack of bugs; with more programmers working on it and more people able to see the source code and spot trouble, problems are fewer and are dealt with much faster when they appear.

When the industry lobbyists told the committee yesterday that “open source” as a concept introduces vulnerabilities, they lied. All the encryption processes your bank and every other use to electronically send billions of dollars around the world are open-source processes; when a computer security system’s workings are completely known yet STILL “uncrackable”, it’s because those processes are “mathematically sound”. We call this stuff “computer science” for a reason.

The process by which the major voting systems companies secure their software NOW is called “security by obscurity”. They build mathematically UNSound systems (often unbelievably so), lie in their product literature about how “state of the art” it all is, and hope that A), nobody else figures out how to hack the hell out of it and B), people don’t realize the obvious counterpart implication that THEY (vendor management and staff) can diddle with election results six ways from Sunday.

Microsoft doesn’t want a major security-oriented application such as voting migrating to open-source (with Linux or similar as the underlying platform) for public relations reasons. And as the 800lb gorilla of the PC software world, they’ve harnessed PC industry figures as their stooges.

Novelist Neal Stephenson has written an essay on the merits of open-source operating systems versus the “Microsoft Dominion” – the discussion of the security implications apply equally well to applications as they do operating systems. It’s...well, LONG, but well written, highly entertaining and worth the read if you really want to understand the issue you’re facing with this resolution and issue: http://laniels.org/weblog/essays/in_the_beginning_was_the_command_line.html

In any case, thank you for at least reading this far ☺,

Jim March