

Jim March
Sacramento, CA
<http://www.equalccw.com/voteprar.html> / jmarch@prodigy.net

Oct. 16th 2003

Mr. Mark Kyle
Undersecretary of State
1500 11th Street
Sacramento, CA 95814

Mr. Kyle,

This letter constitutes my public comments prior to the upcoming meeting of Oct. 28th regarding certification procedures for Diebold's new touchscreen terminal voting system.

More specifically, this letter is actually "part two" – I submitted written comments to Mr. John Mott-Smith's office prior to the meeting of Oct. 9th; according to a published flyer at:

http://www.ss.ca.gov/elections/vsp_100903.pdf

...public comments in writing were to be directed at Ms. Dawn Mehlhaff and as you can see from this reproduction of those comments, that's exactly what I did:

<http://www.equalccw.com/sscomment.pdf>

So if those comments didn't get to the rest of the board, questions must be raised about the proper flow of information negative to Diebold through Mr. Mott-Smith's office. You should also be aware that the numerous visits I paid to that office were spurred by Ms. Mehlhaff's lack of response to my voicemails.

Enough complaints; I will now "get to the point" regarding Diebold and certification.

The first round of comments I submitted (sscomment.pdf above) focused primarily on how Diebold Elections Systems' central vote-count application, "GEMS", has extreme security flaws involving an utter lack of passwords, data security and audit trail security once a the GEMS database is opened (locally or remotely) with an off-the-shelf copy of MS-Access, a common database. That earlier submission on my part showed how Diebold staff mislead the Federally-approved testing lab (Metamor/Ciber) and they were actually surprised they got away with it. You also saw discussions of how MS-Access was being used by Diebold's staff and county-level customers as an "unapproved, illegal hack tool".

There are also references to an internal manual that casts severe doubt on Diebold's corporate ethics.

In this letter, I need to show you what appears to be an even more blatant fraud committed against the Federal testing process.

As you know, “Commercial Off-The-Shelf” (“COTS”) software does not need to be certified. At various times, Diebold has used versions of MS-Windows at both the terminals and central vote-count systems. While I have concerns about the process used to make sure that the NT/2000 series Windows on the GEMS boxes and Win95/98/ME series on the optical scan terminals REMAINS “factory stock”, all of these revisions of Windows are indeed “COTS” per the rules and the lack of specific certification isn’t a legal violation.

One advantage to “COTS” software is that it is possible to prove that the software is un-modified by comparing the as-installed code with the same version bought off-the-shelf somewhere. (Which is why I filed a Public Records Act Request with Alameda County asking for a directory listing of the as-installed files; the county counsel’s office informs me that such a listing is “secret”, a very troubling stance indeed.)

Diebold has declared Windows CE on the touchscreen terminals “COTS” – and THAT is pure fraud.

Windows CE is not a “commercially boxed software product”. It is instead a “development kit” provided by Microsoft to developers of small-scale, limited-functionality computing products. The majority of these are “handheld class” systems similar to a “Palm Pilot”, or advanced cell phones. Because of the extreme variety of hardware that can support CE, Microsoft doesn’t write drivers or other support for the CPU, memory cards/devices, video, keyboard input or the like. In this respect, it is unique among all Windows variants.

Microsoft has extensive technical information on Windows CE which supports this “non-COTS” view of CE:

<http://www.microsoft.com/windows/embedded/ce.net/evaluation/faq/default.asp>

This covers the latest version of CE, which admittedly isn’t being used by Diebold. But the “development process” between CE and CE.net is the same. Read the FAQ, quoting the very first item:

Q. What is Windows CE .NET?

A. Microsoft Windows CE .NET is the powerful, real-time operating system for rapidly building the next generation of smart, connected, and small-footprint devices. Windows CE .NET is the successor to Windows CE 3.0. The latest version, Windows CE .NET 4.2, supports four major CPU architecture families and more than 200 CPU types. It is used in a broad range of device types, including mobile handheld devices, Windows-based thin clients, mobile and Voice over Internet Protocol (VoIP) telephones, gateways, Web pads, digital audio players and receivers, set-top boxes, retail point-of-sale (POS) devices, and industrial controllers. Windows CE .NET is a highly componentized operating system that enables developers to customize an image to meet the specific product requirements across a range of devices.

The rest of the FAQ and the main CE developer's page fills in any remaining blanks:

<http://www.microsoft.com/windows/embedded/ce.net/default.asp>

And as you can see, the entire source code to WinCE is available to Diebold and anybody else, which means Diebold can alter the OS in ways that would be difficult with the true "COTS" versions for which the source code is a closely guarded Microsoft secret:

<http://www.microsoft.com/windows/Embedded/ce.NET/previous/downloads/source/default.asp>

At one point early last year, at least three lower-level Diebold staff realized that CE would need to go for certification:

----- Original Message -----

From: Greg Forsythe

To: Support

Sent: Friday, April 12, 2002 2:28 PM

Subject: Fw: Pennsylvania Certification

Don,

I'm assuming you've got the ball on this.

These are the steps necessary to get started in Pennsylvania. A letter must be sent to Monna Accurti requesting the withdrawal of two previously submitted products with our current products. Completed by Don Vopolensky

The best we can aim for is June certification.

We must submit our request complete with documentation by MAY 1, 2002 for a certification date in June.

We need

1. Win CE 3.0 to be approved by Wylie. Jeff Hallmark says the CE 3.0 will be sent the week of April 15th.
2. GEMS 1-18-9 or better to be go to MetaMore. Already at Ciber
3. Ballot Station 4-3-2 or better to be approved by Will be released Friday, April 12th. Jeff Hintz and Jane Barth to test the hell out it.
4. Certification documentation for GEMS-1-18-9 and BS-4-3-2. Nel Finberg and Tracy Treat documentation progressing. Promised to have it finished
5. Someone to take charge and drive the certification train to Harrisburg. Jeff Hintz or/and Jeff Hallmark

What's next? What else has to be done?

Testing must be done for both OS and TS. Looks like we're going to make it! (Ed.

Note: this paragraph of two lines was enlarged, boldfaced and printed in red in the original.)

Cumberland County has seen all the DRE products and is of the opinion that our product is the best for their needs. Their plan is to use the AccuVote-TS for a few

precincts in November and purchase the system early 2003. They would like to have one DRE for every 250 registered voters. They currently have 127,585 registered voters. 510 AccuVote-TS potential.

Greg Forsythe

That message went to an internal Diebold Email list with approximately 20 to 30 people in the distribution list. One of those people was Talbot Iredale, the head programmer/engineer for Diebold Election Systems, who replied:

To: <support@gesn.com>
Subject: Re: Pennsylvania Certification
From: "Talbot Iredale" <tiredale@gesn.com>
Date: Mon, 15 Apr 2002 09:40:26 -0700
References: <001501c1e269\$1fb16f10\$0e03a8c0@hirondelle>

Don,

We do not certify operating systems with Wyle. Therefore we do not need to get WinCE 3.0 certified by Wyle. What we need to get certified is BallotStation 4.3.2. We do not want to get Wyle reviewing and certifying the operating systems. Therefore can we keep to a minimum the references to the WnCE 3.0 operating system.

Tab

The Emails being cited above are part of the large haul of 1.8 gigabytes of data delivered to Wired Magazine by parties unknown prior to their Aug. 7th 2003 story on the subject. Even if you discount their contents completely, the fact that Windows CE hasn't been submitted for certification is easy for your office to establish. Call up Wyle and Ciber, or the Federal Elections Commission. Or look through your own certification records.

You can then confirm through Microsoft that the Windows CE family is NOT "COTS" within the meaning of the certification rules.

The implications are horrifying. WinCE's uncertified code has access to the screen and data input methods on the terminals, AND access to all of the internal and PCMCIA memory devices storing votes. If anything, this is worse than the "GEMS MS-Access hack" because if the votes are tampered with in an automated fashion at the terminals, not only will the results flowing into GEMS be tampered with, but all three of the data repositories (two at the terminals plus GEMS) will all be consistent.

No recount will be possible. We will have achieved a true "Dieboldocracy".

There is one other problem with the TSX terminal system – in addition to a severe weight-loss program, the TSX allows wireless transmission of elections results. Given Diebold Election System's hideous record in data security to date (read: why does this guy Jim March have their program code and entire Email archive?) this is simply madness.

I'm not the only one who thinks so – Iowa computer scientist Doug Jones has this to say:

The newest version from Diebold, the AccuVote TSX, apparently allows wireless transmission of precinct results to the GEMS server, but Diebold defends this, saying that the electronically transmitted results are only unofficial results, while the official canvass depends on hand-carried records. This subject was discussed in the Acron Beacon Journal on August 15, 2003. [See: "E-voting becomes touchy topic" .at <http://www.ohio.com/mld/beaconjournal/6538203.htm>] Unfortunately, the specific details of canvassing are a matter of state law, outside of Diebold's control, and in addition, the Diebold operating instructions apparently call for the connection to the server to be established prior to computing the precinct totals. This means that the memory cards holding the official results for each precinct are exposed to corruption by any network insecurity, and therefore, that the official canvass can be corrupted if someone hacks into the machine. Furthermore, it is emerging that the version of Windows CE used by Diebold is both heavily customized and full of dynamically loaded libraries. As a result, there are strong grounds for the conclusion that the operating system is not unmodified commercial off the shelf software (COTS), and that with this extensive use of dynamic linkage, we cannot even tell if the system being run on a particular voting machine resembles the system that was disclosed in the configuration documents submitted with this system when it went through the FEC/NASED approval process.

Source: <http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html>

Without adequate security, wireless transmission of results opens an entire universe of vote-hacking. Granted, the hardware/software needed to do wireless data intercept is moderately sophisticated, but not at all impossible and downright simple for any number of government agencies. (Then again, Diebold is already supporting use of cellular modems to transmit results in California, an illegal and uncertified process witnessed directly by poll volunteers in Marin County in the recent recall election. Diebold has played "fast and loose" with the rules so many times, it would take at least 30 pages to make a definitive start at a full accounting.)

In conclusion:

Diebold has slipped at least two major pieces of fraud past the Federal certification process: Windows CE was falsely declared COTS and GEMS has no security whatsoever beyond MS-Windows which the virus problems show is highly defective.

Every Diebold product certified in California must be DE-certified, ASAP. And **then** questions must be asked about the Federal cert process that passed this fraud along to California.

Thank you for at least reading this far,

Jim March

CC: *Mr. Kyle has promised to forward this to the rest of the certification board.
It is also available for public distribution at:
<http://www.equalcew.com/sscomments2.pdf>*