Charles E. Corry, Ph.D.

455 Bear Creek Road
Colorado Springs, CO 80906-5820

Telephone:	(719) 520-1089
Instant Messenger:	drcecorry
Email:	ccorry@ejfi.org
Home page:	corry.ws
Equal Justice Foundation	www.ejfi.org

December 26, 2004

Memorandum

To: Election Assistance Commission (EAC), EAC Technical Guidelines Development Committee (TGDC), Chairs IEEE SCC 38 and P1583
From: Charles E. Corry, Ph.D., F.G.S.A., President, Equal Justice Foundation
Re: IEEE standards project P1583 Standards for Voting Equipment

Standards for vote counting equipment

For more than three years I have been actively involved with the IEEE P1583 voting equipment standards committee, testified repeatedly as an expert witness on computer voting in court and before the Colorado legislature, worked as a precinct election judge, had numerous discussions with local election officials, and written extensively on this topic. However, I have not found convincing evidence that computers, whatever their other benefits, provide a secure, trustworthy, cost effective method of counting ballots.

The most fundamental problem and objection to the use of computers, or any machine, to count ballots is that such equipment completely, and seemingly unavoidably eliminates the fundamental protections provided by the oversight of the ballot counting process by citizen election judges and poll watchers of diverse backgrounds and affiliations.

One of the principal failures of the current standards development is that no underlying bedrock principles have been defined that such standards must follow. Thus, we have been building the house before the foundation. I have included my own poor efforts for proposed voting principles on the latest version of the P1583 draft. I would urge both the EAC and IEEE to adopt basic and universal voting principles before going further.

I know of no instance where the standard engineering practice of making a cost/benefit analysis has been performed with regard to the use of computers for counting votes. As we use paper ballots that could as easily be hand counted as optically scanned, in the medium-sized county where I live the use of vote counting computers adds at least $1 for every vote cast in every election, or an additional expense of about $300,000 per election. The Caltech/MIT study suggests that computer vote counting may become cost effective in election jurisdictions with more than 25,000 active voters. If that estimate is valid it would rule out the use of computer voting in all but a handful of counties in Colorado on a cost basis alone, as well as most of the sparsely-settled regions of the western United States.

To my mind the integrity of our elections is of more fundamental and critical importance than military security. Yet the security measures and testing procedures currently undertaken by voting equipment manufacturers and election officials would be laughable if they weren't so critical to the future of this nation. And, in my experience, Colorado election officials have repeatedly refused to permit an outside review of their procedures though we have many of the best computer security experts in the country here. When independent security reviews have been run, notably in Maryland and Ohio, the results were frightening. Additionally, when an IT election official was arrested for theft and fraud in Denver shortly after the November 2003 election, no attention was paid to the security issues.

The issue of security is a major deadlock in the IEEE P1583 standards committee. Present voting equipment has the security of a Game Boy toy. To add the requisite security will greatly increase the cost, which everyone recognizes. Manufacturers are aware that cost/benefits for computer voting are marginal now, at best, and that increased costs for essential security does not work in their favor. So we can have cheap, insecure voting machines, or we can have expensive, marginally secure vote counting machines. Neither is a good option in my opinion as the physical security of vote counting machines in most election districts is appalling and already a number of them have been stolen or "lost."

The probability that any Microsoft Windows-based voting equipment has been invaded by viruses, Trojan horses, hack tools, keystroke loggers, spyware, and etc., is exceeded only by the probability that local election

Fellow, Geological Society of America
Marquis Who's Who in the World, 16th — 21st Editions
Marquis Who's Who in America, 53rd — 59th Editions
Marquis Who's Who in Science and Engineering, 4th — 8th Editions
Marquis Who's Who in the West, 27th — 32nd Editions
2000 Outstanding Scientists of the 20th Century
2000 Outstanding Scientists of the 21th Century—First Edition
Strathmore's Who's Who, 1998-1999 and 2000-2001 Editions

officials have not taken adequate precautions against hacker intrusions and are in denial about the problems. I presently know of no way to prevent such invasions with a Windows OS, particularly with unsophisticated users such as election officials. Therefore, I would strongly recommend that Microsoft operating systems **not** be certified for use in any voting equipment.

Computer vote counting equipment is quite sophisticated. Conversely, election officials are almost universally technologically unsophisticated. Thus, even if the vote-counting computers contained open-source software, only a few of the largest election districts can afford to hire their own voting equipment IT professionals. As a result, when computers are used in an election, the programming and maintenance must be contracted out at considerable expense. However, a citizen boarding an airplane today goes through a more rigorous background and security check than does a technician hired by voting equipment manufacturers to service voting computers in actual elections. There isn't even a requirement that such technicians be American citizens or reside in this country legally. And voting software is known to have been developed and modified by foreign nationals and most computer hardware is built in a foreign country.

There does not appear to be good evidence that electronic voting as presently envisioned and implemented provides significantly better access to voting for most handicapped individuals than previously existing methods, even if we ignore the increased costs of computer voting. Field tests in actual elections have elicited many complaints from blind voters. Thus, the touted justification of easier access for handicapped voters currently rests on very shaky ground. Therefore, I see no valid justification for using computers to count votes at present.

Standards for central tabulation and ballot generation equipment

I note that the IEEE SCC 38 committee has not made any attempt to date to begin development of standards for central vote tabulating equipment. Yet there is where the greatest potential for election fraud lies. Why attempt to hack hundreds of individual voting machines when in a few seconds one can change the election results of an entire county at the central computer? And the gross security problems with Diebold's GEMS software have been widely published. Thus, the critical problem of development of standards for central vote tabulating and ballot generation equipment is being left by default to NIST and the TGDC. I am not sanguine about that development, particularly in the brief time period available. Therefore I urge the IEEE to immediately initiate a working group to develop standards for central vote tabulation and ballot generation computers under SCC 38 in cooperation with NIST, and that the EAC adopt only interim standards for this equipment until a more formal process can be completed.

Standards for statewide voter registration databases

There is a similar situation with regard to standards for the statewide voter registration databases mandated by HAVA. It is likely the development of a secure yet readily and rapidly accessible relational database with adequate referential integrity will be one of the most difficult and time consuming HAVA requirements. The present process for implementing such a database in Colorado is probably a perfect example of how *not* to do this. That is particularly apropos since our Sec. of State, Donetta Davidson, serves on the TGDC. First, attorneys with no discernible technological training or database experience are in charge of the development. Secondly, development has been contracted out to a discredited company, Accenture, that is based offshore. Third, the declared intent is security by obscurity and outside review is not invited, wanted, or allowed. Fourth, Ms. Davidson is in the habit of appointing Blue Ribbon oversight committees whose members have no technical background and the only technical input sought or received is from vendors. In my professional experience this is a perfect recipe for failure.

Again I would urge the IEEE to immediately initiate a working group under SCC 38 to develop standards for such statewide voter registration databases in cooperation with NIST. In the meantime I would ask that the EAC adopt only interim standards for this equipment until a more formal process can be completed.

Conclusions

The computer vote counting equipment currently in place is worse than simply another multibillion dollar fraud perpetrated on American citizens, it threatens the very basis of our democratic society. This is not to say that computers have no place in elections but *I do claim that currently deployed vote counting equipment is not deserving of the trust of the American people.* Hand counted paper ballots provide a viable, time-tested method for secure elections with established trust of the citizenry, particularly in small election districts where computer voting is never likely to be cost effective.

Before proceeding further down the electronic voting path I would urge the IEEE and EAC to implement rigorous standards for central vote tabulating and ballot generation equipment, and statewide voter registration databases with security based on a far more substantial basis than obscurity and refusing to allow citizen review.

Rushed, divisive voting equipment standards without strong security provisions are worse than no standards at all, and would tend to provide a false sense of security and trust unjustified by facts and research.