Douglas W. Jones
Department of Computer Science
University of Iowa
Iowa City, IA 52242
phone: (319) 335-0740
Fax: (319) 335-3624
E-mail: jones@cs.uiowa.edu

March 20, 2003

The Honorable Kevin Shelley
Secretary of State
1500 11th Street
Sacramento, CA 95814
Fax: (916) 653-3214

Dear Sir:

I have learned that you have convened an ad hoc committee to study security issues raised by the widespread use of Direct Recording Electronic or DRE voting machines.

These issues have concerned me for many years; I have served for a decade on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems, and I recently completed three terms as chair of that board. My interest in issues surrounding voting machines has led me from an initial concern with security issues to a broader interest in human factors and administrative issues surrounding their use, and as a result, I have been called on to speak before numerous audiences about many aspects of voting technology, including the United States Civil Rights Commission (2001), the House Science Committee (2001), and the Federal Election Commission (2002).

As a computer scientist, my expertise is in the area of operating systems, including real-time systems and embedded systems, and in parallel discrete event simulation; my work in embedded systems has had several practical spinoffs, including a braille computer printer, a robotic pan-tilt-zoom camera mount that is currently patented and commercially available, and a handicapped accessible optical mark-sense voting system, currently patent pending. I have also developed algorithms that have been used for image compression, cryptography, scheduling and simulation.

Voting technology is something like the elephant in the old Indian folktale, and many of us are like blind men studying that elephant. One of us feels the legs and

describes it as a tree, focusing on the need for physically robust voting machines that can survive long-term storage, rough transport and occasional bursts of intense use. Another of us feels the trunk and describes it as a snake, focusing on the user interface, human factors and administrative needs, while yet another of us feels the ear and describes it as a great shelter from the rain, focusing on security and reliability issues.

I want to emphasize that the entire elephant must be addressed, voting systems must meet security, usability and physical durability standards, and an attempt to say, as some have, that there is a single number-one issue in voting system design are surely mistaken!

Last year, I sat on a panel at the WEST02 conference convened by Ted Selker, where we discussed human factors problems, and I have emphasized these problems in written and oral testimony before several groups. Human factors and administrative issues were at the center of the debacle in Florida back in 2000, almost all involving older voting technologies based on punched-card and mark-sense ballots. In their rush to replace those older systems, Florida demonstrated in 2002 that similar mistakes could also be made with the newer generation DRE voting systems.

While I continue to be intensely interested in these human factors issues, I want to emphasize the fact that DRE voting systems introduce new and unparalleled security problems, and that we must not let the pervasive human factors problems with all of our voting technologies distract us from the need to address these!

It is important to remember that every change in voting technology has created new avenues for election fraud. While our democracy has, on the whole, thrived, it has done so despite widespread but scattered instances of election fraud; some big city political machines have been notorious in this arena, but it has not been difficult to find rural areas with equally corrupt election practices. Invariably, the examples are 10, 50 and 100 years old, and invariably, it is fair to say that today, most jurisdictions are honest and conscientious; despite this, it is evident that the crooks have always been there to exploit the weaknesses of whatever voting system we use.

It is irresponsible to introduce a new voting technology without close attention to the vulnerabilities of that technology, and where we can easily identify how such fraud could be perpetrated, we must arm ourselves against it. Generally, new voting systems are not the targets of fraud until they have been in use for long enough for the crooks to learn their weaknesses, and until they are used widely enough for these weaknesses to be worth exploiting.

While there have been allegations of fraud surrounding DRE voting systems, until recently, DRE systems have not been widely enough used to be worth subverting. This is no longer true, and with the recent funding of the Help America Vote Act, DRE systems will become pervasive enough to become primary targets for election fraud.

With the previous generations of voting technologies, it was widely understood that the primary weaknesses involved ballot box stuffing at the precinct level, deliberate miscounts in canvassing at the county level, and doctoring of voting machines at the county level; as a result, the most common election frauds involved local and county races. Today's DRE systems make those attacks difficult, but the centralized development of software for these machines creates a new vulnerability: A crook who buys the services of the right person can now attack elections at the state or national level in a way we have never before experienced! The potential gain to a successful crook who carries out such an attack is immensely larger than the potential gain to a crook who attacks at the precinct or county level, and therefore, even though such an attack may be less likely, we must be vigilant in our defense.

It may be possible to focus excessively on fraud! After all, most of the problems with our election systems stem not from malice but from simple mistakes, and this is as true of the software written for DRE systems as it is in all other areas of election practice. On the other hand, it is also important to notice that the very same controls we place on our systems to prevent fraud also catch the vast majority of accidental mistakes. It is an old maxim of computer security that whatever damage could be done by one deliberate attacker can also be done by some combination of careless but well intentioned programmers and users, and this seems to apply equally well to the realm of elections.

It is important to understand that, while the NASED/FEC standards have long required that all DRE systems maintain something called an audit trail, this audit trail does not record the one thing that a bank examiner, for example, would expect to find there: a record of the votes. As a result, unlike the audit trails represented by the paper receipts and internal cash register tape maintained by an ATM, the audit trails of all but a few DRE machines on the market today offer no assurance that the votes were recorded as intended by the voter, and offer no possibility of a meaningful challenge to the honesty of the machine in the event that fraud may be suspected. This is unconscionable!

I have heard several vendors tout the impossibility of a recount as one of the great advantages of DRE systems, and I certainly understand why election administrators hate recounts and may find this attractive. Human factors experts also point out that accurate recounts are notoriously difficult to conduct, and they are correct.

On the other hand, the risk of an election system that is inherently unauditable are entirely unacceptable. To address this, I have long advocated routine manual audits of all elections, not in the form of total recounts, but in the form of a carefully conducted hand recount of one randomly selected race in one randomly selected precinct after every election. In addition to maintaining statistical quality control over whatever election technology is being used, this practice maintains a corps of election workers with experience in conducting and administrating recounts, ready for those rare occasions where a more general recount is required.

It has been argued that the software audits conducted under the FEC/NASED process should be enough to assure us that the software in our DRE systems is honest. I disagree! I have read the FEC/NASED software source-code audit reports for every machine brought before Iowa's board of examiners since these became available to us, and I have seen too many systems that had evident flaws despite their FEC/NASED seal of approval; I am happy to say that none of these was a deliberate flaw. I have also seen plenty of evidence that our software audits do catch many flaws, so my overall conclusion is that our current FEC/NASED certification process, while seriously flawed, is still quite valuable.

I signed Dr. Dill's petition asking for a voter-verified paper audit trail recording each ballot cast because I believe that this technologically simple scheme allows us to make an end run around many of the problems with the current FEC/NASED certification process. I would like to see less expensive solutions to the same problem, but these will involve far stronger and much more difficult to explain security technologies, such things as capability based computer architectures and cryptographic technology, and while I have high hopes for these methods, we must not wait for them before we demand genuinely auditable elections. We must not allow the current generation of unauditable DRE systems to become as pervasive as punched cards or optical mark-sense ballot scanners.

Sincerely:

Douglas W. Jones
Associate Professor of Computer Science