

Board of Examiners for Voting Machines and Electronic Voting Systems between 1994 and 2004, and I chaired that board for 3 years from 1999 to 2002.

4. I have testified on issues related to voting technology before the District Court of the City and County of Denver Colorado in *Conroy vs Dennis* on September 20-22, 2006, before the Supreme Judicial Court of Maine *In the matter of primary election ballot dispute 2008* on July 7, 2008 and before the US District Court for Eastern Pennsylvania in *NAACP vs Cortes* on October 28, 2008.
5. As Michael Shamos has testified, I have recommended the use of parallel testing to augment the security of electronic voting systems. Nonetheless, there are stronger defenses, noteworthy among them is post-election auditing of hand-marked paper ballots after optical mark-sense scanning.
6. My recommendations are included in my Tutorial on *Testing Voting Systems*, reprinted as Appendix E of *The Machinery of Democracy: Protecting Elections in an Electronic World*, Brennan Center for Justice at the NYU School of Law, June 27, 2006. This tutorial is available on the Internet at:
<http://www.cs.uiowa.edu/~jones/voting/testing.shtml>
7. As Michael Shamos has indicated, parallel testing can be accomplished in a variety of ways, some of which give significantly more assurance than others.

8. I described this variety in *Parallel Testing: A menu of options*, a report prepared for the Miami-Dade County Elections Department on August 12, 2004. This report is available on the Internet at:
<http://www.cs.uiowa.edu/~jones/voting/miamiparallel.pdf>
9. (This report is specific to the iVotronic voting system from Election Systems and Software. Replace the terms *PEB* and *CF card* with the generic term *electronic storage media* to make the report apply broadly to other voting systems.)
10. In my tutorial on parallel testing, I said that it addresses "some of the security questions that have been raised about Direct-Recording Electronic voting machines." I want to emphasize the word some.
11. Parallel testing does not address all of the security questions that have been raised about direct-recording electronic voting machines. Specifically, parallel testing cannot generally detect malicious software or firmware that only functions after being awakened by a *secret knock*.
12. The term *secret knock* refers to a pattern of inputs used to trigger malicious behavior that is provided, perhaps unwittingly by voters or pollworkers after the polls are opened.
13. Dishonest software or firmware, for example, might be written so that it only misbehaves after a particular name is

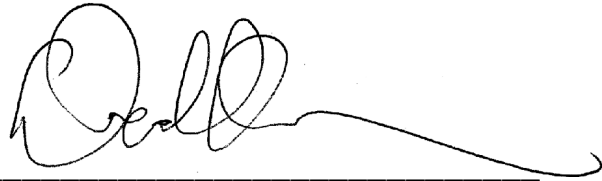
entered as a write-in candidate in some minor race on the ballot. A word of mouth campaign to get people to write in that name could suffice to trigger misbehavior in many precincts.

14. Designing parallel tests to discover secret knocks is generally impossible, although there is always a very remote possibility that a secret knock could be discovered by accident.
15. This is why I recommend the use of post-election auditing, to the extent that the voting system permits such audits.
16. When a direct-recording electronic voting system is used without a voter-verifiable paper audit trail, post election auditing is a weak defense, and the security of the system is significantly strengthened by the use of parallel testing.
17. Where there is a voter-verified paper audit trail printer attached to a direct-recording electronic voting machine, post election auditing becomes a much stronger tool, but parallel testing remains useful.
18. The reason for this is that about two thirds of all voters do not check the printout created for the audit trail. I base this approximate number on laboratory studies I am aware of at Rice University and on surveys conducted by the news media after the first deployment of voter-verified paper audit trails in Nevada.

19. Both parallel testing and post-election auditing can also be applied to the scanners used to tabulate optical-scan mark-sense ballots.
20. In the context of optical-scan mark-sense ballots, post-election auditing is significantly stronger than parallel testing for two reasons.
21. First, with hand-marked paper ballots, the vast majority of voters watch to see if their marks appear on the ballot as they intend. This does not guarantee correct interpretation, but as the data from the 2008 Minnesota Senatorial Recount indicates, the vast majority of voters do correctly understand the ballot marking instructions and make marks that are scanned as intended.
22. Second, in an audit of hand-marked paper ballots, the percent of voters who mismark the ballots in a manner that cannot be read by the scanners can be directly observed, while we have very poor tools for recognizing whether voters on direct-recording electronic voting machines are confused. There is ample circumstantial evidence, however, that such confusion has played decisive roles in elections, for example, in the 2006 election to Florida's 13th Congressional District.
23. This leads to my opinion that optical mark-sense scanning of hand-marked paper ballots with routine post-election auditing is the strongest voting system currently available. In my

opinion, this is stronger than direct-recording electronic voting machines with routinely audited voter-verifiable paper trails and parallel testing. In turn, these are stronger in my opinion than direct-recording electronic voting machines with parallel testing or direct-recording electronic voting machines with routinely audited voter verified paper audit trails, and either of these are stronger than direct-recording electronic voting machines with neither defensive measure.

24. I certify that the foregoing statements are true. I am aware that if any statements are willfully false, I will be subject to punishment.

A handwritten signature in black ink, appearing to read 'Douglas W. Jones', written over a horizontal line.

Dated: April 6, 2009
Iowa City, Iowa

Douglas W. Jones