



California
VOTING SYSTEMS AND PROCEDURES PANEL MEETING

April 21, 2004, Sacramento California

**Prepared testimony of Cindy A. Cohn, Legal Director
of the Electronic Frontier Foundation**

I would like to thank the panel for the opportunity to address you on this important topic. The Electronic Frontier Foundation (EFF) believes that the very integrity of our democracy is at stake in this debate and that California must ensure not only that our voting systems work, but that they work in an openly verifiable manner. My remarks will address Agenda items 1-3. While they are somewhat separate, I believe that they can be best addressed together and together paint a very clear picture of what decisions need to be made to ensure a secure and accessible vote for the November election.

In brief, while EFF was supportive of the Secretary of State's original decision to require voter verified paper ballots by 2006, we now believe that the combination of Diebold Election Systems' wholesale failure to abide by the rules requiring escrow and certification of election systems and the significant and widespread difficulties experienced in the March 2, 2004 election across several paperless election systems, should compel this Panel to recommend to the Secretary of State that he:

1. Immediately decertify all election equipment that does not contain a voter verified paper audit trail ("paper trail"), by which I mean a system that creates a permanent paper record that is made available for inspection and verification by the voter at the time the vote is cast and preserved within the polling place. The fourteen California counties that have already purchased equipment that does not currently have a paper trail may use their optical scan systems -- that they use for absentee voting -- if they cannot acquire equipment that creates a paper trail in time for the November elections.
2. In order to ensure full, secure and private accessibility for disabled and non-English speaking voters, the Secretary should require the counties who cannot provide an alternate means for accessible, private voting for those individuals to petition the Secretary of State for a one-time waiver of this requirement. The waivers shall allow non-paper-trail systems for disabled and non-English speaking voters in locations where specially trained election officials can ensure that the systems function properly and correct any problems in a timely fashion. At a minimum, the systems at these locations should be tested and used in accordance with the recommendations of the RABA report.¹

¹ RABA, *Trusted Agent Report Diebold AccuVote-TS Voting System*, January 20, 2004:
http://www.raba.com/press/TA_Report_AccuVote.pdf

Background on EFF

The Electronic Frontier Foundation (EFF) is a San Francisco-based nonprofit public interest organization dedicated to protecting civil liberties and free expression in the digital world. With over 12,000 paying members, EFF represents the interests of the public both in court cases and in the broader policy debates surrounding the application of law in the digital age. EFF opposes misguided legislation and agency regulation, initiates and defends court cases preserving individual rights, launches global public campaigns, introduces leading edge proposals and papers, hosts frequent educational events, engages the press regularly, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to websites in the world, www.eff.org.

EFF has long been involved in computer security issues, including handling the litigation that released encryption technology from federal government control – a necessary first step to its use in computerized voting machines. EFF has also been deeply involved in the nationwide discussion about computerized voting machines for the past year. Our specific activities include:

- Counsel to the Professors Aviel Rubin, Daniel Wallach and others who authored the Johns Hopkins/Rice University report on the security flaws in the Diebold voting machines issued in August, 2003.
- Plaintiffs' counsel in *Online Policy Group v. Diebold*, which resulted from the company's attempt to misuse the copyright "cease and desist" notices to stop publication of embarrassing internal e-mails, including messages where employees suggested that the company "charge up the ying yang" should a Secretary of State require voter verified paper ballots. Diebold permanently withdrew its cease and desist letters as a result of the litigation.
- Following the computerized voting machine standards as they are developed at the Institute of Electrical and Electronics Engineers (IEEE) Standards Association.
- Assisting with litigation arising from computerized electronic voting machines nationwide, including the current dispute in Riverside County arising from a request for a reasonable recount by Linda Soubrious.
- Assisting with litigation nationwide arising from security problems with computerized election systems.

The Secretary of State Should Decertify

As mentioned above, EFF was supportive of the Secretary of State's decision to require paper trails and other security measures by mid-2006. Events since then, however, have demonstrated that the security dangers, as well as practical difficulties arising from use of computerized voting

machines, are much worse than we had known. These have reluctantly led us to conclude that the computerized voting machines without paper trails must be decertified immediately.

As to agenda item 1, concerning Diebold, this panel is well aware that Diebold completely failed to abide by basic security requirements throughout the state. The state election code contains two fundamental checks to ensure that the systems Californians vote on have not been tampered with. First, it requires that all election systems, *in whole or in part*, be certified prior to any use. California Secretary of State Voting System Certification Procedures, section 102 (“Procedures”). Second, it requires that a complete copy of any election system used in the state be deposited into escrow. Procedures, section 1601 and 1824 (requires all changes to be deposited in escrow). The certification requirement ensures that the code works as advertised and falls within at least a minimum level of robustness and security. The deposit requirement ensures that the State can check for tampering – if investigation of a machine after an election demonstrates that the code it runs varies from the escrowed code, the machine has been improperly altered. It is now established that Diebold violated both of these requirements, putting the security of the March 2 election (and probably prior elections) in jeopardy. And they did so in every single Diebold voting machine used in the state. This was no momentary lapse or emergency situation, breaking California election law was apparently business-as-usual at Diebold. I am quite familiar with ordinary software development processes and recognize that ongoing releases of updates and patches are commonplace for mass marketed software. But the same is not true for critical machines running sophisticated, mission-critical software and is certainly not true for machines where maintaining the integrity of the code and system must be maintained. Both of these are true for election machines.

As to agenda item 2, it is now clear that widespread technical problems with electronic voting systems caused massive disenfranchisement during the March 2, 2004 election. In Alameda County, problems with Diebold smart card encoders impacted one-fourth of the county's polling places;² in San Diego County, encoder problems impacted nearly 40 percent of the county's polling places.³ Thousands of Orange County voters were given the wrong electronic ballots; many were unable to cast votes in contests for which they were eligible, while others were allowed to vote in districts in which they did not reside.⁴

In urging the Secretary of State to decertify, we are sensitive to the requirements of the disabled and non-English speaking communities and believe that ensuring accessible voting must remain a paramount concern. We believe, however, that any attempt to construe this discussion as trade-off between secure and accessible voting presents a false choice. It is as unnecessary and inappropriate to require all voters to risk flawed elections in order to ensure accessible voting as

² Ian Hoffman, “E-voting probe finds no reason for glitches,” Oakland Tribune, April 13, 2004: <http://www.oaklandtribune.com/Stories/0,1413,82~1865~2080543,00.html>

³ Helen Gao, “Faulty switches cited in voting woes,” San Diego Union-Tribune, April 14, 2004: <http://www.signonsandiego.com/news/metro/20040414-9999-6m14diebold.html>

⁴ Stuart Pfeifer, “Mult-Precinct Polls Blamed for Mix-Up, Los Angeles Times, March 21, 2004: <http://www.verifiedvoting.org/article.asp?id=1652>

it is to assert that secure voting must be inaccessible. While the long-term solutions are more elegant, we believe that for purposes of the November 2004 election these important voters can be reasonably accommodated in the counties that have purchased computerized voting machines lacking paper trails. For some, this may mean “conditionally certifying” assistive technologies that allow accessible voting on optical scan and other equipment. For counties that use Sequoia machines, machines with paper trails will be certified and deployed in Nevada in time for the elections. It may be possible to secure sufficient numbers of these to allow one machine per polling place as required by the Help America Vote Act.⁵ We suggest that the Secretary of State assist counties in locating and, if necessary, sharing paper trail capable equipment, whether optical scan or otherwise.

If none of these solutions are appropriate for a particular county, we suggest that counties be allowed to petition the Secretary for a one-time, limited waiver of the decertification order in order to allow some voting on computerized voting equipment that does not contain a voter verified paper ballot. The waiver would allow a county to create specific locations for use of such machines by the disabled and non-English speaking communities as long as these locations are staffed by election officials with significant knowledge and experience in managing and trouble-shooting the machines in general and specific training about how to assist disabled people and non-English speakers in using the machines. We also suggest that the Secretary require that any such machines comply with additional security measures, at a minimum those suggested in the RABA report.

Conclusion

EFF applauds Secretary of State Shelley on the courageous steps he has taken so far to ensure secure voting in California. As the nation’s leader in developing secure technologies for the world, we are proud that California has led the nation in ensuring that computerized voting systems are secure, verifiable, accessible and trustworthy. Unfortunately, the computerized voting machines being used and sold in California today plainly fail to meet those basic standards, and the risk of injuring our democracy is too great for us to simply cross our fingers and hope that the significant problems we have experienced so far will not recur in November. Accordingly, based upon the problems with computerized voting machines to date, we believe that the only way to ensure this is to immediately decertify all computerized voting machines that do not contain voter verifiable paper ballots and to take the steps outlined above to ensure that Californians enjoy accessible, verifiable and secure voting in November.

⁵ Help America Vote Act section 301 (a)(3)(B)