



▼ ADVERTISING

I can use Western Union to send money by

WESTERN UNION

westernunion.com

washingtonpost.com > Metro > Maryland > Government

Jolted Over Electronic Voting Report's Security Warning Shakes Some States' Trust

By *Brigid Schulte*
Washington Post Staff Writer
Monday, August 11, 2003; Page A01

The Virginia State Board of Elections had a seemingly simple task before it: Certify an upgrade to the state's electronic voting machines. But with a recent report by Johns Hopkins University computer scientists warning that the system's software could easily be hacked into and election results tampered with, the once perfunctory vote now seemed to carry the weight of democracy and the people's trust along with it.



enlarge photo

Newer computerized voting machines were used in four Maryland counties in elections last year. All states are required to update equipment by 2006. (Michael Robinson-chavez -- The Washington Post)

▼ ADVERTISING

Join millions of singles here.

Personals on
washingtonpost.com

powered by match.com

An outside consultant assured the three-member panel recently that the report was nonsense.

"I hope you're right," Chairman Michael G. Brown said, taking a leap of faith and approving Diebold Election System's upgrades. "Because when they get ready to hang the three of us in effigy, you won't be here."

Since being released two weeks

ago, the Hopkins report has sent shock waves across the country. Some states have backed away from purchasing any kind of electronic voting machine, despite a new federal law that has created a gold rush by allocating billions to buy the machines and requiring all states, as well as the District of Columbia, to replace antiquated voting equipment by 2006.

"The rush to buy equipment this year or next year just doesn't make sense to us anymore," said Cory Fong, North Dakota's deputy secretary of state.

The Local Count

THE DISTRICT

The District replaced its antiquated punch-card machines with an optical scan voting system in 2002. D.C. officials plan to spend \$8.5 million in federal and local funds to purchase Sequoia Direct Edge electronic voting machines. The District plans to put one such machine in each of its 142 precincts before the 2004 election to comply with the Help America Vote Act. The law requires that by 2006, each precinct have a handicapped-accessible machine.

MARYLAND

In 2001, the state split the \$13 million cost with Montgomery, Prince George's, Allegany and Dorchester counties to buy 4,678 Diebold AccuVote-TS electronic machines. State officials recently signed an agreement worth up to \$55.6 million with Diebold to buy 11,000 more of the machines, which would go in every

Maryland officials, who signed a \$55.6 million agreement with Diebold for 11,000 touch-screen voting machines just days before the Hopkins report came out, have asked an international computer security firm to review the system's security. If they don't like what they find, officials have said, the sale will be off.

The report has brought square into the mainstream an obscure but increasingly nasty debate between about 900 computer scientists, who warn that these machines are untrustworthy, and state and local election officials and machine manufacturers, who insist that they are reliable.

"The computer scientists are saying, 'The machinery you vote on is inaccurate and could be threatened; therefore, don't go. Your vote doesn't mean anything,' " said Penelope Bonsall, director of the Office of Election Administration at the Federal Election Commission. "That negative perception takes years to turn around."

Still, even some advocates of the new system are thinking twice. The Leadership Conference on Civil Rights, which pushed for electronic machines to help visually impaired and disabled voters, says the Hopkins report has given them pause. They're calling on President Bush and members of Congress to convene a forum of experts to hash it out. "We have become concerned about these questions of ballot security," said Deputy Director Nancy Zirkin.

Her group and others supported passage of the \$3.9 billion Help America Vote Act in November. Of the \$1.5 billion appropriated so far to replace old machines, rewrite outdated equipment standards, encourage research to improve technology, train poll workers and update registration lists, about half has been released. And that has all gone toward buying electronic machines, which cost as much as \$4,000 a piece.

"These vendors are everywhere," said David Blount, spokesman for Mississippi Secretary of State Eric Clark. "They're besieging everyone."

The remaining money is to be released once an Election Assistance Commission is appointed. By law, the board was to have begun work in February. But the names of the four commissioners, two from each major party, have yet to go to the Senate for confirmation.

The stakes are high. The 2000 Florida presidential election showed the shortcomings of the current system.

A subsequent Cal Tech/MIT report found that of more than 100 million votes cast nationwide, as many as 6 million weren't counted because of registration errors or problems with punch-card and lever machines. One study found that of 800 lever machines tested, 200 had broken meters that stopped counting once they hit 999.

Frustrations with the old machines -- levers were invented in the 1930s and punch cards in 1904 -- have turned many local election officials into staunch

precinct in the state. After the 2000 presidential election, a state task force, convened by then-Gov. Parris N. Glendening (D), recommended that the state use one unified voting system with electronic machines.

VIRGINIA

Cities and counties determine which machines to buy. They are then tested and certified by the State Board of Elections. Four cities and counties in Virginia, including Charlottesville and New Kent County, have modern touch-screen electronic voting machines. Alexandria uses an optical scanning machine. Arlington and Fairfax counties use older electronic equipment but are negotiating to buy Advanced Voting Solutions' latest wireless touch-screen machines. Norfolk is the only place in Virginia using Diebold electronic machines.

— Government IT News —

- [Happy Anniversary, E-Government](#) (washingtonpost.com, Dec 18, 2003)
- [Pentagon Boosts High-Tech Tagging](#) (The Washington Post, Dec 18, 2003)
- [White House Web Scrubbing](#) (The Washington Post, Dec 18, 2003)
- [More Government IT News](#)




— Message Boards —

- [Post Your Comments](#)

— Free E-mail Newsletters —

- [News Headlines](#)
- [News Alert](#)

Subscribe to *The Washington Post*

-  [E-Mail This Article](#)
-  [Print This Article](#)
-  [Permission to Republish](#)

▼ ADVERTISING

TOP JOBS *from local employers*

- [SALES REPRESENTATIVE. AT HOME. /](#)
- [Sales Representative/ Hitech Instruments](#)
- [Writers | Editor/ Tqm](#)
- [Technical lead/ Planet Assoc](#)
- [Work from home - Online](#)

supporters of the new electronic models. Advocates for the disabled say that the machines will enable the visually impaired, for the first time, to put on headphones and vote a secret ballot.

[accountant/ Sunrise Co.](#)

[All Top Jobs](#)

Mischelle Townsend, registrar of voters in Riverside County, Calif., said the electronic machines have saved as much as \$600,000 in paper every election and, from 1996 to 2000, helped increase voter turnout to 72 percent, up 10 percent.

Any tampering would be caught, she said, in the extensive pre- and post-election testing. The best defense of the machines, she said, is that there has been no documented case of voter fraud. "If the computer scientists had one valid point, one, then why hasn't one incident of what they're saying occurred in all of these elections?"

But past is not prologue, historians and political scientists warn.

"Some of these hacking scenarios are highly improbable. But it's not completely out of the question," said Larry J. Sabato, a political scientist at the University of Virginia who has written about political corruption. "When the stakes are high enough in an election, partisans and others will do just about anything. So this is a worry."

Bugs, Glitches Can Abound

Computer scientists note that computers are unreliable, subject to bugs, glitches and hiccups as well as the more remote possibility of outright hacking and code tampering.

They warn of a hostile programmer inserting what they call Trojan horses, Easter eggs or back doors to predetermine the outcome. They point to a number of errors in the 2002 elections, from poll workers -- like some in Montgomery County -- unfamiliar with how long it takes to warm up the machines to mysterious vote tallies.

In Georgia, where Diebold machines are used, a handful of voters found that when they pressed the screen to vote for one candidate, the machine registered a vote for the opponent. Technicians were called in and the problem was fixed, state officials have said.

In Alabama, a computer glitch caused a 7,000-vote error and clouded the outcome of the gubernatorial race for two weeks. But more critically, computer scientists charge that the software that runs the machines is riddled with security flaws.

"Whoever certified that code as secure should be fired," said Avi Rubin, technical director of the Information Security Institute at Johns Hopkins and co-author of the report.

Rubin analyzed portions of Diebold software source code that was mistakenly

left on a public Internet site and concluded that a teenager could manufacture "smart" cards and vote several times. Further, he said, insiders could program the machine to alter election results without detection. All machines had the same password hard-wired into the code. And in some instances, it was set at 1111, a number laughably easy to hack, Rubin said.

Because there is no paper or electronic auditing system in the machine, there would be no way to reconstruct an actual vote, he said.

In a 27-page rebuttal, Diebold dismissed the findings. Officials said that the software Rubin analyzed was old and that only a portion may have been used in an actual election. "Right now, we're very, very confident about the security of our system," said Mark Radke, a Diebold executive. "If there is a way to make it more secure, we're open to that from good, reliable, knowledgeable sources who don't have a previous agenda."

That doesn't satisfy some critics. "The most important thing about the Hopkins report is not the security holes they found, but irrefutable proof that all this stuff that the machines are secure is hot air," said David Dill, a computer scientist at Stanford University who has turned the debate over electronic machines into a national crusade.

State and local election officials, however, say the checks and balances -- the poll workers and judges, the thick manuals of procedures -- ensure the sanctity of elections.

"It's not fair to do an evaluation that doesn't talk about context," said Mary Kiffmeyer, president of the National Association of Secretaries of State. "Our voting process has all kinds of security. It's not just the box of technology."

Few Players in Game

Although free and fair elections are a central tenet of America's democracy, no one paid much attention to how they were executed for years. Not until 1990 did federal elections officials decide to write voluntary standards to certify voting machines.

Still, the atmosphere remained fairly clubby, with one lab doing the testing and a revolving door between voting machine companies and the state officials who later went to work for them. Although nearly 20 companies have had equipment certified by the FEC, only three are major players: Diebold, with 55,000 touch screens throughout the country; ES&S of Omaha; and Oakland, Calif.-based Sequoia Voting Systems.

All machines go through the FEC's testing and certification process, which can cost companies anywhere from \$25,000 to \$100,000. Yet a 2001 report by the General Accounting Office found that the FEC standards do not thoroughly test for security or user friendliness and that only 37 states follow them.

Doug Jones, a computer scientist in Iowa, said the testing is so secret that even

he, as an insider who serves on the state board that certifies voting equipment, can't get information. Five years ago, he found the identical security flaws cited in the Hopkins report.

"They promised it would be fixed," Jones said. "The Hopkins group found clear evidence that it wasn't. Yet for five years, I had been under the impression that it was fixed."

Diebold's Radke said the code has been fixed.

Even the most vocal critics say there are workable solutions. Computer scientists say the companies should release their secret source codes for expert review, as two start-ups, VoteHere and Populex, have agreed to do. Or that states should require automatic upgrade clauses, as Santa Clara County has.

Dill, the Stanford computer scientist, and others are pushing for what are called voter-verified audit trails. By attaching a printer to every machine, voters can review the electronic ballot before it drops into a locked box.

Many solutions are already spelled out in the Help America Vote Act, which mandates tougher security, usability and accuracy standards.

In the end, however, with experts still at loggerheads and the 2004 election looming, voters are left wondering which side to trust. Howard A. Denis (R-Potomac-Bethesda), a Montgomery County Council member, was so shaken by the Hopkins report that he is considering asking for a waiver to stop using electronic machines.

"The more I look into this, the more serious I think it is," he said.

© 2003 The Washington Post Company

Navigate to News Sections 

Navigate the Metro Section 

washingtonpost.com

PRINT EDITION | [Subscribe to The Washington Post](#)



[NEWS](#) | [OPINION](#) | [SPORTS](#) | [ARTS & LIVING](#) | [ENTERTAINMENT](#)

[Discussions](#) | [Photos & Video](#) | [JOBS](#) | [CARS](#) | [REAL ESTATE](#)

washingtonpost.com: [Contact Us](#) | [About washingtonpost.com](#)
[E-mail Newsletters](#) | [Archives](#) | [Wireless Access](#) | [Media Center](#) | [Advertise mywashingtonpost.com](#) | [Our Headlines on Your Site](#) | [Rights and Permissions](#)
[Make Us Your Home Page](#) | [Work at washingtonpost.com](#) | [Internships](#) | [Site Index](#)

The Washington Post: [Subscribe](#) | [Subscriber Services](#)
[Advertise](#) | [Electronic Edition](#) | [Online Photo Store](#)

The Washington Post Co.: [Information](#)
[Other Washington Post Co. Websites](#)

SEARCH: News Web by  

[Member Agreement and Privacy Policy](#) | © Copyright 1996- 2003 The Washington Post Company