

OPERATION ENDURING VOTE

This is a call to Americans.

Not Republicans, not Democrats, not Greens, not Libertarians.

Americans.

It is a call to Americans to protect our country and to protect our most essential right—
The right to cast our votes and to have those votes determine the future of our nation.

We now face a grave threat to our elections, one which can make your vote disappear into untraceable electrons—where it will be impossible to determine if your vote and the votes of your fellow citizens were accurately cast and counted.

In the past few elections, many counties and states have begun the use of paperless electronic voting systems. They're slick. They're easy to use. And they pose a serious threat to the accountability of our voting system, because most of these machines produce no printed record of your vote.

Here's why many of the country's **top computer [security experts are sounding the alarm about paperless electronic voting machines \(EVMs\)](#)**:

1. EVMs do not produce a paper ballot, so
2. EVMs don't let you verify a hard-copy paper ballot before your vote is cast, which means—
3. EVMs make manual recounts impossible, and therefore
4. EVMs make many machine errors irreversible and untraceable.

5. EVMs also usually contain court-protected secret software and
6. EVMs are prone to software and mechanical errors.
Finally—
7. EVMs are vulnerable to fraud, and [Stanford's Dr. David Dill](#) says that
8. Even rigorous testing of EVM software can't reveal malicious programs that could subvert an election.

The [New York Times](#) and [Wired Magazine](#) and [Salon.com](#) and [MSNBC.com](#) have all run a number of articles on the potential problems of paperless electronic voting. Websites like [verifiedvoting.org](#) and [notablesoftware.com/evote](#) and [blackboxvoting.com](#) reflect a rapidly rising concern about the problems of electronic voting. This comes during a growing chorus of reported computer security complaints—according to [the November, 2003 report on Electronic Voting by the Congressional Research Office](#) over 100,000 in the last year alone.

So the irony is that the electronic voting machines, which are being frantically forced into action in response to the anger and confusion of the 2000 Presidential recount in Florida could bring worse voting security problems than the chad-based voting systems they will replace.

But the worst damage from an ill-considered rush to new and unproven electronic voting technology could be to the already shaky trust of American voters.

One of the most recent and glaring examples of untraceable voting machine error was suffered by Republican incumbent Fairfax, VA School Board member, Rita S. Thompson. A [Washington Post story](#) on November 6, 2003 quoted Thompson.

"It's hard not to think that I have been robbed," said Thompson, when county officials tested one of several electronic voting machines that seemed to have malfunctioned during the election and "discovered that it seemed to subtract a vote for Thompson in about 'one out of a hundred tries.'"

Thompson's "77,796 recorded votes left her 1,662 shy of reelection. She is considering her next step, and said she was wary of challenging the election results: 'I'm not sure the county as a whole is up for that. I'm not sure I'm up for that.'"

Computer Security Scientist, [Dr. Rebecca Mercuri](#), had this to say about this event: "Regarding the November 2003 Fairfax, VA election, we have no proof that the election results are correct or incorrect, because there is no way to perform an independent recount of the ballots. It is clear, though, that a number of the machines were defective, since the County discovered that some votes could have been subtracted. This situation provides a good illustration of how voter verified paper ballots could have been helpful in resolving questions that arise following election equipment malfunctions."

While the nature of electronic voting makes it impossible to assess whether or not Thompson was "robbed," Ms. Thompson's (and the voters') inability to know what happened to her votes points out the ever present danger of paperless electronic voting. In a contested election, given no ballots to recount, you just run the computer totals again and get exactly the same results, and everyone goes home hoping, and not knowing, that the computer didn't mess up. And if an electronic voting system does fail and reverse an election, the subverted election will still stand because there's no paper trail to recount.

This is no way to run a democracy.

So, since her complaint is almost certainly futile without a paper ballot trail to use in a recount, Rita Thompson may choose not to act, but that doesn't mean that we can't.

There is a way out of the long, dark road of unverified computer voting and it is in your hands to make it happen: The latest buzz out of Washington, DC., may offer us a way to stop the nightmare of untraceable votes and irreversible computer voting errors. It is called

[Operation Enduring Vote](#)

The information on Operation Enduring Vote follows.

For the Republic and our democracy,

Steve Corrick
Operation Enduring Vote
gardenearth@aol.com
www.operationenduringvote.com

OPERATION ENDURING VOTE

[Operation Enduring Vote](#) is one part of the campaign to save the printed, voter-verified ballot—and with it, the integrity of the American election system.

To do so, we need to force the US Congress to pass [Rep. Rush Holt's HR 2239](#). HR 2239 is a bill to Require All Voting Machines To Produce A Voter-Verified Paper Trail. It ensures that election officials are required to have a permanent, easily readable record of your votes in the event of ballot counting problems, or an election recount, or in the event of suspected election tampering.

The following shows that Congress is already getting strong constituent feedback on verified voting. One prominent congressional staffer offers this insight. "Members of Congress from both parties are saying that the topic that comes up most in their Town Hall meetings with constituents these days—second only to the Iraq conflict—is HR 2239, Rep [Rush Holt's](#) bill to require all electronic voting machines to produce voter verified paper trails." Holt's Bill demands several basic changes in existing election law:

1. It requires that, BEFORE the 2004 election, all voting machines produce a voter verified paper record for use in audits and recounts.
2. HR 2239 bans the use of undisclosed software and wireless communication devices in electronic voting machines.
3. 2239 speeds up the implementation of electronic voting for the handicapped, and,
4. Finally, Holt's bill requires an automatic .5% random recount of all election results to ensure that there were no ballot irregularities. (A summary of Holt's bill is available at: <http://holt.house.gov/issues2.cfm?id=5996/>)

How to Hold Congress' Feet to the Fire on 2239. At this writing, there are [82 Representatives](#), (16 in the last nine days as of 11/23/2003), who have agreed to co-sponsor HR 2239. However, HR 2239 is buried in the House Committee on Administration, by the Committee's Chairman, Rep. Bob Ney of Ohio (18th District), and the bill has little chance of receiving a vote unless we act now. But Congress will recess for the Holidays in early December, so time is critical. Here's what we can do.

1. Find out who your local Representative and your two local Senators are. If you don't know, you can get their contact information at <http://www.Congress.org>. Also [see the webpage on Verified Voting that shows how your congressional representative stands](#) on HR 2239.
2. Then call each of their offices NOW and ask for the exact schedule of when and where the Congressperson/ Senator is holding open town meetings in his/her home district during the winter recess. *Get their schedule first.* If you cannot get it from the staff person, go to the congressperson's website at <http://www.house.gov/> or <http://www.senate.gov/> to see if they have upcoming service days in their district when they will be in a local office near you. Also see if they have coffees or morning gatherings for constituents, on a weekly basis in their DC offices.
3. Once you've gotten the schedules, ask them how they stand on Rush's bill. If they don't know or won't tell you, let them know that you support it and that you and your colleagues will be publicly asking them to support it.

4. **We'll be there for HR 2239.** Let the staffer know that you plan for yourself or other supporters of HR 2239 to go to every event the Congressperson holds in his/her home district and that you will publicly ask the Representative or Senator to support 2239. Let them know you also plan to bring the media to the events so that there will be press coverage of the Congressperson's replies to the issue.
5. If you cannot talk to them directly, send them [email](#), [letters](#) or [faxes](#) with the message, **"We'll be there for HR 2239."**
6. Send this letter to everyone you know will also support protecting our Democracy and the accuracy of every American's vote. Encourage them to follow the process above.
7. Contact all of the organizations you know which have expressed interest or support for a voter verified paper trail. Some of these include: [the Democratic National Committee](#), the [National Federation of Republican Women](#) and [the Communication Workers of America](#). Ask them to notify their membership of Operation Enduring Vote and to also contact their Representatives and Senators.

Verified Voting Talking Points: When you go to a public meeting, here are a few key facts to bring up that your representative may not know:

1. In 2000 [voting machine problems forced Venezuela to shut down](#) its entire national election and to reschedule it for several months later because of problems with the voting machines from ES & S, the biggest voting machine company in the US.
2. The companies say that they cannot produce accurate paper printouts but Diebold has already produced and sold over [300,000 voting machines to Brazil , which produce a printed ballot](#) for every voter.
3. Diebold's machines have been examined in [reports from two independent computer security groups](#). Computer security scientists from Johns Hopkins University said in a July 24th New York Times article that within the first 30 minutes they found "major, major flaws" in the Diebold security that would not be acceptable for a freshman-level computer security programmer. Science Applications International Corporation confirmed numerous failings, including the lack of tampering and fraud protection and the lack of capacity for recount.
4. Leading national computer professionals and security experts have stated clearly in a [Resolution on Verified Voting](#) that **computer voting systems cannot be made completely secure**. They have formally recommended that any electronic system have a verifiable paper audit trail as the only way voters can have confidence that their vote has been recorded correctly each time, and so that recounts and spot checks are possible. The Resolution on Verified Voting is at <http://verifiedvoting.org/resolution.asp>

The links underlined in this document are online at <http://www.gardenearth.com/operationenduringvote>

How Can We Know We're Still a Democracy Without a Permanent Printed Ballot of Your Vote?