APPENDIX

New Jersey should switch to optical scan voting

Andrew W. Appel

October 2017

Almost all NJ's counties use paperless DRE (direct-recording electronic, "touchscreen") voting machines. Because these voting computers have no paper trail that could detect and correct computer hacking, New Jersey's counties should switch now to a more trustworthy voting method used by most states: precinct-count optical scan voting.

By background, I am a computer scientist with expertise in computer security and formal verification of software. But for the last 15 years I have also studied, and written about, elections and voting technology.

Andrew W. Appel

Professor of Computer Science

Princeton University

Precinct-count optical-scan

Optical-scan balloting was introduced in the U.S. about 1970. By the 1980s, precinct-count optical scan was already in use in some places. In the precinct-count system, the voter marks the ballot and feeds it directly into the scanner in the polling place. The computer (in the white box on top) counts the votes, and the ballot drops into a sealed ballot box (the blue box at bottom). With well designed ballots, precinct-count optical scan has proved to be a very accurate and trustworthy way of voting.

New York (Essex County) opscan ballot 2016

OFFICE	DISTRICT ATTORNEY (Vote for ONE)	COUNTY CORONER (Vote for TWO)	SUPERVISOR (Vote for ONE)	TOWN CLERK (Vote for ONE)	TOWN COUNCILMAN (Vote for any TWO)		SUPERINTENDENT OF HIGHWAYS (Vote for ONE)	TAX COLLECTOR (Vote for ONE)
Democratic A ★			Archie R. Depo		Kate Comegys Mongulla	Robert Segall	Kevin R. Zaumetzer	Susan J Richards
Republican B ★	Kristy L. Sprague	Francis W. Whitelaw		Beatrice A Pelkey	John J. Sheldrake	Amy F. Shelton	John F. Pulsifer, Jr.	Lori A. Ducharme
Conservative C	Kristy L. Sprague							
People's D							William H. Lincoln	
Cowboys E							Kevin R. Zaumetzer	
Friendship F						Robert Segall		
Spencer Reynolds G					Spencer Reynolds			
Fair Deal H							Erin R. Himmel	
Honesty I					John J. Sheldrake			
Write-in	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN

3

Those New Yorkers, putting the offices across the rows and the parties down the columns -- any New Jerseyan knows it should be the other way around! Which you can do, of course, on an opscan ballot.

Touch screens:
Direct-Recording Electronic
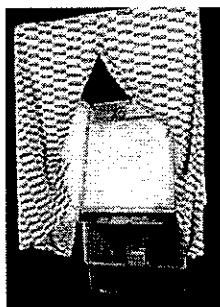
Shouptronic, 1980

Sequoia, 1987
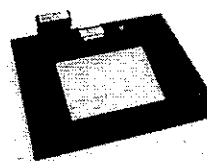
Votronic, 1991

Sequoia, 2000

Diebold, 2002

4

In the 1980s and 1990s, voting-machine vendors developed "direct-recording electronic" (DRE) voting computers. In this system, the voters indicate their choices on a touchscreen (or some other input device), and the computer records and counts the vote in its internal memory, and/or in an electronic memory cartridge. There's no paper record of the vote (but see note below). At the closing of the polls, the machine can print a cash-register-tape printout of the results; this along with the memory cartridge are transported to a central place for aggregation (adding up all the per-machine totals).

After the polls close, the machine can print out a list of every vote cast, from its internal memory; but that's not the same as a paper ballot that the voters can see, and if the computer is wrong (by accident or cheating), then the paper is just a printout of those wrong numbers.

Some DRE voting computers (in about 3 states of the U.S.) are outfitted with a "Voter Verified Paper Audit Trail" that the voters *can* see before they cast their vote, and that drops into a sealed ballot box that can be recounted by hand. That's an important check on the computer memory; but it still has many problems: most voters don't understand what that printout is for; and they don't check it very reliably; the thermal paper ("cash register tape") is hard to recount by hand. Better technology is now available, for example, voters that are unable to use pen-and-paper can use touch-screen Ballot Marking Devices (BMDs) that can produce optical-scan ballots to be counted by op-scan voting machines.

4✓

Ballot definition files
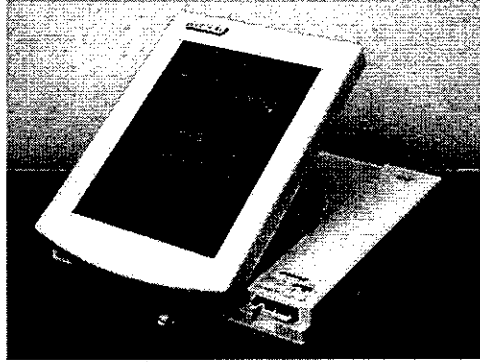
How does the computer program in the voting machine "know" what candidates are on the ballot? The answer is that there is a "ballot definition file" prepared by election administrators, listing all the contests and candidates.

Election Management computer

GOVERNOR
[ ] John Smith
[ ] Mary Jones
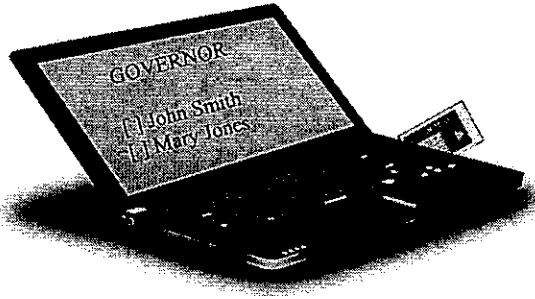
Ballot Definition
Cartridge

6

The election administrator (a county employee, or a contractor, etc.) uses software on an ordinary laptop or desktop computer to prepare the ballot definition file. Then the ballot definition is written to a removable memory cartridge (like a thumbdrive, or some similar technology). This is the "ballot definition cartridge."

Ballot definition files

Insert memory card
into the PCMCIA
slot of a voting machine
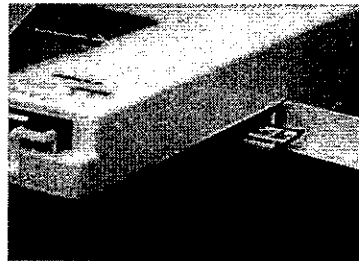
7

The ballot definition cartridge is then inserted into a slot on the voting machine. Here, you can see that the slot is down low on the right-hand side. Now the voting computer is ready for election day.

Fundamental flaw of voting computers:

Whoever programs the computer,

decides what election results are reported by the
computer program inside the voting machine

8

'nuff said.

How to commit election fraud

- Write a computer program that
  - On nonelection days, accurately counts votes
  - On election days, between 8:00 a.m. and 5:00 p.m., cheats: adds votes to the wrong column
  - Voter won't see anything amiss
  - Nor will pre-election "logic and accuracy" testing!

- Load your program into voting machines
  - At the factory, or
  - In the field

9

Suppose someone wants to steal an election by hacking a voting machine. They can replace the legitimate vote-counting program inside the voting computer, with a fraudulent program that deliberately miscounts the votes. If you were doing this, you wouldn't make it *always* cheat, because the election administrators sometimes test the machines, before the election, by casting a few votes and then seeing the total. This is called "logic and accuracy testing," or LATA. LATA is good for some things—for example, making sure that the touchscreen isn't miscalibrated, or that the ballot definition is generally OK.

BUT, it's easy to make a cheating vote-stealing program that isn't detected by logic and accuracy testing! Every voting machine (just like any other kind of computer) has an internal clock, so it knows when it's election day. So you just make your cheating program cheat only on election day, after 8am. Since the LATA is done *before* election day, the cheating program will be on its "best behavior" when LATA is done.

Here's how to install a vote-stealing program into one of NJ's AVC Advantage voting machines
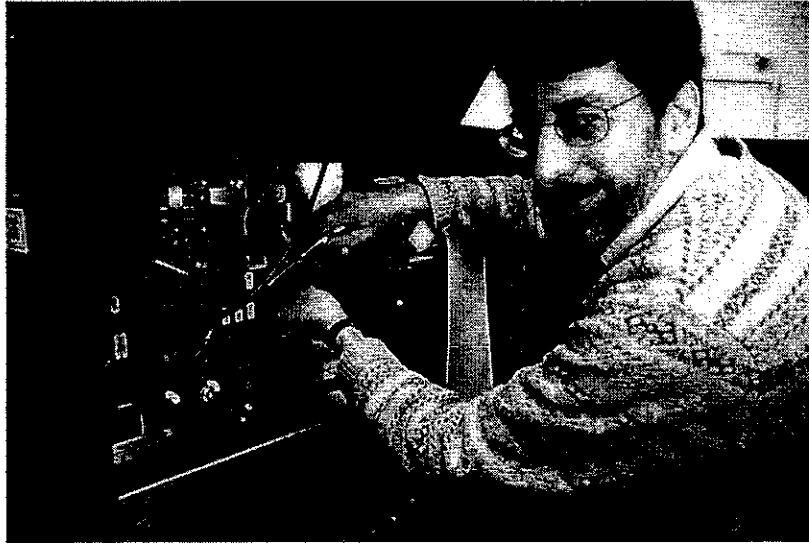
(This machine is still used in NJ, LA, PA)

Then, to install that vote-stealing program in the AVC Advantage voting machine, I picked the lock on the back door of the machine. That's easy, it's a cheapo lock; I'm not at all an expert lock-picker, but I can pick this lock in about 10 seconds. Then I unscrew 10 screws on the panel that covers the motherboard. You can see the motherboard here, it's green. Those four computer chips with the white labels on them, hold the computer program that runs the election. Just replacing one of them, at lower right, is enough to install my vote-stealing program. The whole process takes about 7 minutes, using a screwdriver.

By the way, you might think that the state could install some tamper-evident security seals, and that would prevent the crooks from getting in there. But you would be wrong! Supposedly "tamper-evident" seals don't provide much protection. See my paper, "Security Seals on Voting Machines: A Case Study," by Andrew W. Appel. *ACM Transactions on Information and System Security,* vol. 14, no. 2, pages 18:1--18:29, September 2011.

> ## Selected technical conclusions
> Regarding the AVC Advantage voting machines used in NJ,
> from my testimony in Gusciora v. Corzine, NJ Superior Court, 2009
>
> - Reverse-engineering the program: ~25 person-weeks
>   - If you get a copy of the source code: 1 week
> - Writing the program that cheats: 2 days
>   (122 lines of source code)
> - Time to install fraudulent ROM: 7 minutes
>   - pick lock: 10 seconds
>   - unscrew 10 screws: 2 minutes
>   - pry out ROM, press in new: 1 minute
>   - replace screws: 3 minutes
>
> - Tamper-evident seals can *all* be defeated
>
> 11

In connection with my expert-witness testimony in a court case in New Jersey (2008-2009), I did a forensic examination of New Jersey's "AVC Advantage" voting machines. As part of that study, I wrote a vote-stealing program. First, my team had to understand how the legitimate program works, before modifying it to cheat. This is called "reverse engineering." We tried it two ways: first, without the "source code," and second, with the "source code." It's much easier with the source code, of course, but either way it's well within the capabilities of a moderately qualified hacker.

Then, writing the vote-stealing program is easy—it took just a couple of days to write and test.

By the way, don't try this at home! It's a felony to install vote-stealing programs into a government owned voting machine that will be used in an election. I did mine as part of a court-ordered forensic study, inside a secure building at the New Jersey State Police headquarters. But an election hacker wouldn't have that kind of respect for the law.

Firmware that cheats

✓ Don't cheat in Pre-LAT mode

✓ Cheat only when at least N votes cast

✓ Modify "audit*trail" consistently with vote totals

✓ Modify in-cartridge results consistently with internal-memory results

- Don't cheat until polls open at least 10 hours

- Don't cheat except on election day

- Don't cheat if time/date very recently changed

- . . .

12

Here are some things my vote-stealing program did, so as to avoid detection. Basically, it waits until 8pm when the pollworker turns the key to shut down the election and print out the results. Just before printing out the results, my program shifts 20% of the votes from candidate A to candidate B. The computer program stores the votes redundantly in two different memories, so my program makes sure to cheat in both memories. The computer program has an "audit trail" in its electronic memory that's supposedly some sort of protection, so my computer program changes the audit too!

By the way, the Ballot Definition File has each candidate listed with his/her party affiliation (Democrat or Republican). So if you want to steal votes generically in favor of one party or the other, it's easy to program that up. Once you install that program in the voting computer, it will steal votes in election after election for many years to come.

On more "modern" voting computers,
How do you replace the software?
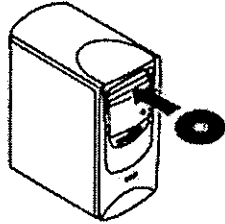
Load it from CD-ROM,   or USB

or download from Internet
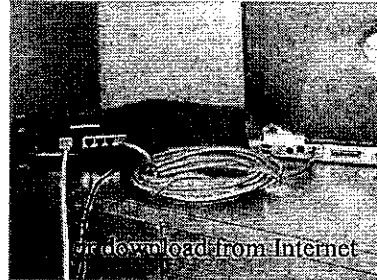
Or, insert memory card
into the PCMCIA
slot of a voting machine
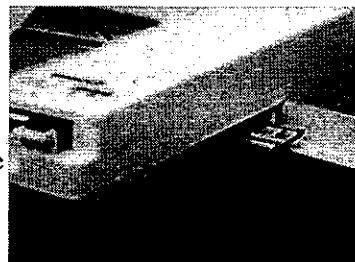
13

On most voting computers these days, you don't need a screwdriver to replace the vote-counting program. It's loaded in on a memory card, a removable media like a thumbdrive or the equivalent. In fact, on most voting machines, you use the same memory-card slot where the Ballot Definition Cartridge is inserted. If you put a card into that slot, that *instead* of the ballot definition, has a new vote-counting program, then the computer will replace its old vote-counting program with your new one.

13✓

Anyone with physical access . . . .

. . . can hack a voting machine
by inserting a card.

Insert memory card
into the PCMCIA
slot of a voting machine
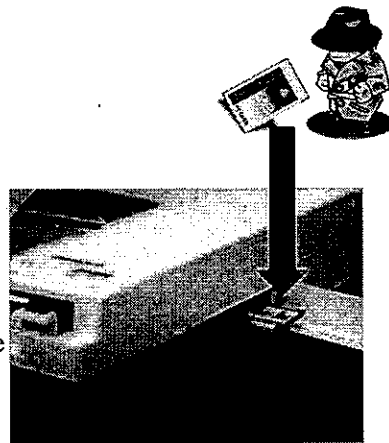
14

And therefore, if you can get unobserved access to a voting machine for just a minute or so, you can install vote-stealing software into it.

Between elections, voting machines are stored in warehouses. County employees have access to them, to perform maintenance such as replacing batteries. I'm sure 99.9% of those public servants are trustworthy and of the highest integrity. But we organize our elections so you shouldn't have to trust every single election worker. That's why there are witnesses in the polling places, and witnesses to recounts, and so on.

Right before an election, voting machines are delivered to the polling places: school gymnasiums, firehouses, churches, town-hall lobbies. There, in many cases, they are left unattended and unsecured. Anyone could get access to those machines and stick in a cartridge.

And what about *after* an election, before the voting machines are collected from the polling places? Hacking them at that point won't change the election that just happened, but it will make the machine cheat in the *next* elections, for years to come.

To steal a big election, the attacker would have to install cheating software in many voting machines, not just one. But surely that's well within the capabilities of a corrupt political machine—or even a freelance criminal who steals votes in favor of a candidate who's not even aware of the fraud.

Voting machine is hackable (indirectly) from the Internet.
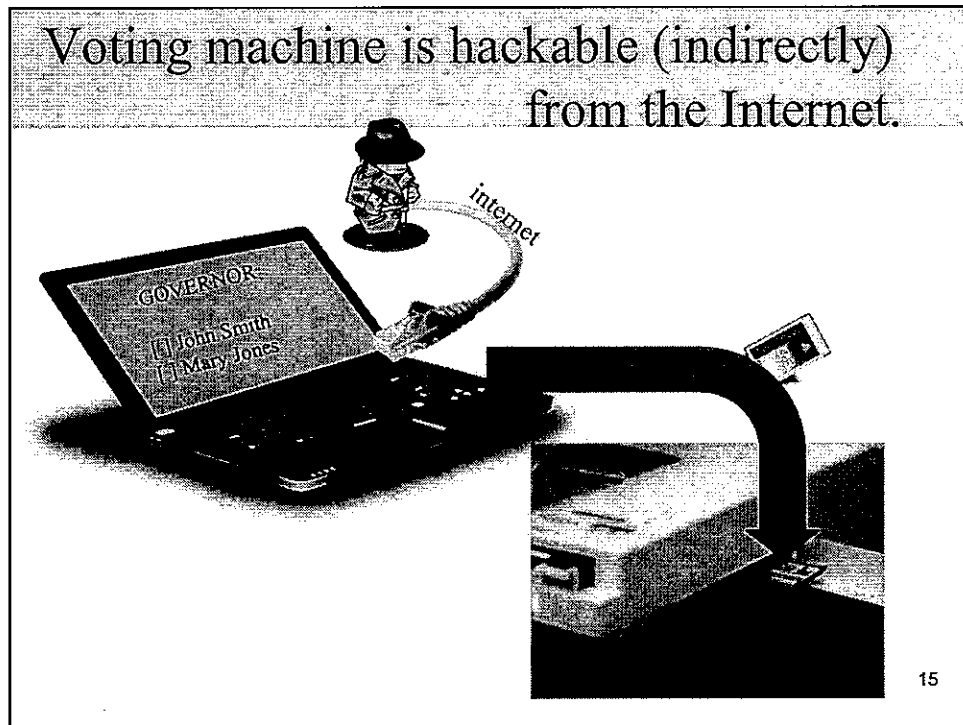
An election administrator may say, "our voting machines don't connect to a network, so they can't be hacked from the Internet." That's not true: even if a voting machine has no network connector, it *can* be hacked from the Internet.

And here's how to hack a voting machine from the Internet. The attacker hacks in to the election administrator's network, and gains access to the computer used for programming Ballot Definition Files. He hacks that computer so that, in addition to putting Ballot Definitions into the removable cartridge, the election management system computer also writes a fraudulent vote-counting (vote-stealing) program to the cartridge. The computer will put the vote-stealing program into every Ballot Definition cartridge destined for every voting machine. Then, when that cartridge is loaded into the voting machine, before the election, it will be installing the vote-stealing program.

This attack was first demonstrated in 2006, on a real voting machine:

Security Analysis of the Diebold AccuVote-TS Voting Machine, by Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07),* August 2007.

New Jersey's AVC Advantage computers cannot have a new vote-counting program installed from removable media (except as regarding their "audio kit"); but hackers can still switch candidates around on the Ballot Definition file and make them correspond to the wrong locations on the screen.

Hox

If the Ballot Definition doesn't match the paper overlay,
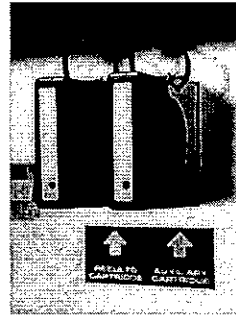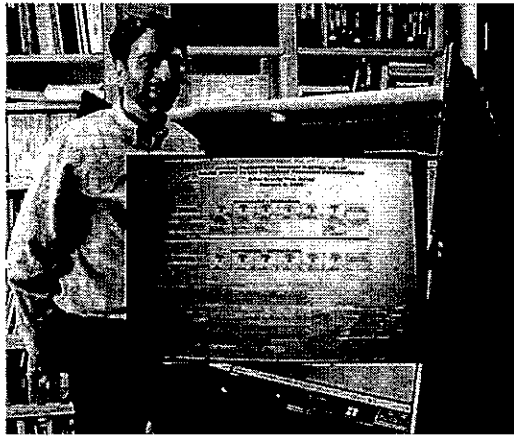
then you're voting for a different candidate than you think!

16

If the Ballot Definition doesn't match the paper overlay,
then you're voting for a different candidate than you think!

This actually happened in New Jersey!
(Finding of fact by Judge David E. Krell, Superior Court of NJ,
in *Zirkle v. Henry,* Docket No. CUM-L-000567-11, 2011.)

Was the swapping of positions by accident, on purpose, or through hacking?
Hard to tell, because a Cumberland County elections technician erased
the evidence, one day before the scheduled forensic examination.

Judge Krell wrote, "I do not know and may never know exactly why this election was
defective. I have suspicions that something happened here that was improper and I
even question whether something happened here that may have been criminal."

17

Conclusion: hackability of voting computers

Computers connected to the Internet, *even indirectly*, can be vulnerable to hacking.
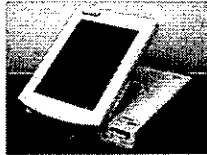
Election officials should use good security practices to make their computers *less vulnerable*, but there is no way to make them *invulnerable*.

Therefore we should run our elections in a way that can detect and correct for computer hacking, without having to put all our trust in computers.

18

And therefore,

Don't use paperless touch-screen voting computers!
They are a *fatally flawed* technology.

And actually, everybody knows this now:

Only a few states still use them.
One by one, states are switching to optical-scan.
Since 2004, no states have switched *to* paperless voting.

19

States that used paperless DREs in 2016

States where almost all voters or most voters use paperless DREs

20

About 10 states still use paperless direct-recording electronic (DRE) "touchscreen" voting computers, for most or all of their voters. Two or three states use touchscreen DREs with a "voter verified paper audit trail," which is not quite as bad. About 37 states use optical-scan balloting for almost all their voters.

Hand-counted paper ballots?

- Works well in many countries
  - where there's just one contest on the ballot

- **In U.S. elections, has a major flaw:**
  - **So many contests to count**
  - **hand counting difficult to do accurately**
  - difficult to find volunteers from both (all!) parties to supervise against cheating

21

Even by 1900, people noticed that it's hard to count paper ballots by hand. Actually, in Europe or Canada, it's not so hard, because in their parliamentary, nonfederal systems they have elections with only one contest on the ballot. And then you can count by hand, by just sorting the ballot papers into one pile for each candidate, and counting up the piles. But in an American election, there are many contests on the same ballot: President, Senator, Congressman, Governor, State Senator, State Rep., Mayor, Councilman, School Board, Dogcatcher, Judge retentions, propositions. To count those, at 8pm after a long election day, is hard to do consistently and accurately.

Precinct-count optical scan voting
(used in most states)

Voter marks op-scan ballot

Voter feeds ballot to scanner

22

Here's a better idea: Voters mark their choices on a paper ballot, and feed the ballot into an optical-scan computer that counts it accurately.
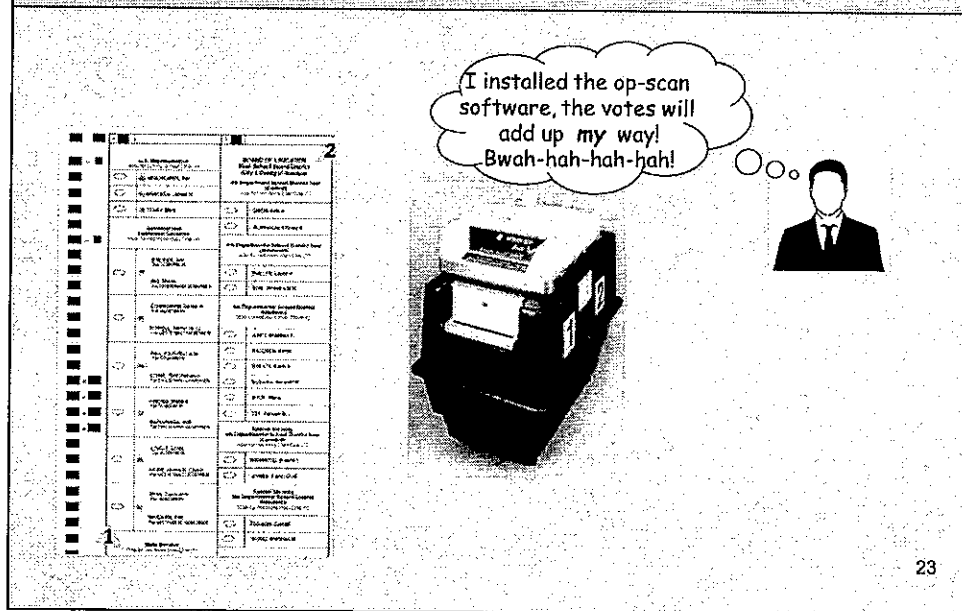
Well, that is, the op-scan computer counts it accurately *if the computer has not been reprogrammed to cheat!* So, why is that any better than a touchscreen DRE?

Voter-Verified Paper Ballot

"Voter Verified" means:
The voter sees the actual
votes, on the *ballot of record*
that will be used for recounts,
without any computer in the way.

Voter marks
op-scan ballot

Voter feeds
ballot to
scanner

Rats!

Paper ballot
drops into
ballot box

Ballots can
be recounted
by hand

24

Here's why: You can recount the paper ballot *that the voter actually marked* by
hand, in the presence of witnesses from both parties, without any computer
"interpreting" the ballot to you.

Random audits

- If you have to recount the ballots by hand, what's the point of having a computer?

- Solution: Recount a random sample of precincts!
  - If there's widespread computer fraud in many precincts, recounting paper ballots in just a few precincts will find evidence of a discrepancy

  - Besides "recount a random sample of the ballot boxes," there are other cost-effective methods for making "risk-limiting audits" a standard part of all elections prior to certification of final results.

25

These audits help protect *not only* against cheating inside the voting computer. They also protect against accidental miscalibration, accidental mistakes in the layout of the Ballot Definition File, and so on.

Some states do audits

Paper ballot audits, 2018
- No audits
- Weak audits
- Audits (but needs improvement)
- Excellent audits

Source of data: Verified Voting Foundation   Map: Appel, using mapchart.net

26
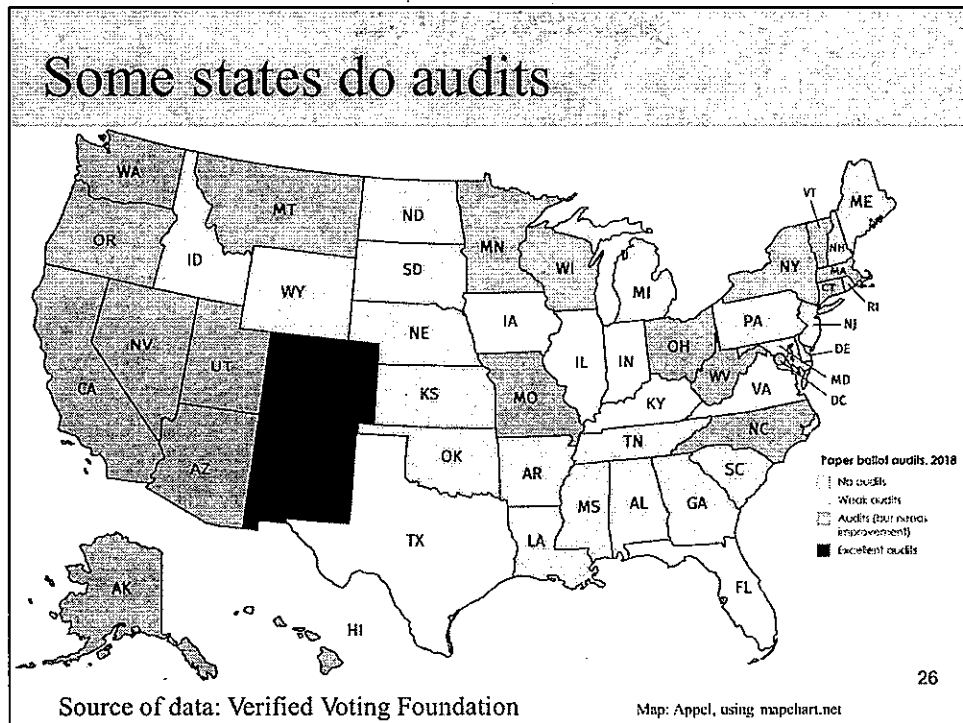
A few states do random audits, but unfortunately,

1. Not very many states do it (just the ones shown here in light green and dark green)

2. Even in most of the states that do audits, the audits are inadequate. They don't audit enough percentage of the ballot boxes to catch fraud (if it were to occur); or they do the audits *after the results are officially certified,* when it's too late; or they don't audit the actual paper ballots, which means that a cheating computer could still fool them.

Audits are the best way to protect against computerized election theft, but they have to be done well in order to provide protection. Colorado and New Mexico have models that other states should emulate.

Note: some states (IN, PA, NJ) have statutes requiring audits, but most of their voters use unauditable paperless DREs, so in practice they don't do ballot audits.

Conclusion: hackability of voting computers

Computers connected to the Internet, *even indirectly*, can be vulnerable to hacking.

Election officials should use good security practices to make their computers *less vulnerable*, but there is no way to make them *invulnerable*.
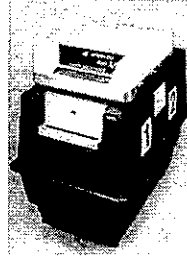
Therefore we should run our elections in a way that can detect and correct for computer hacking, without having to put all our trust in computers.
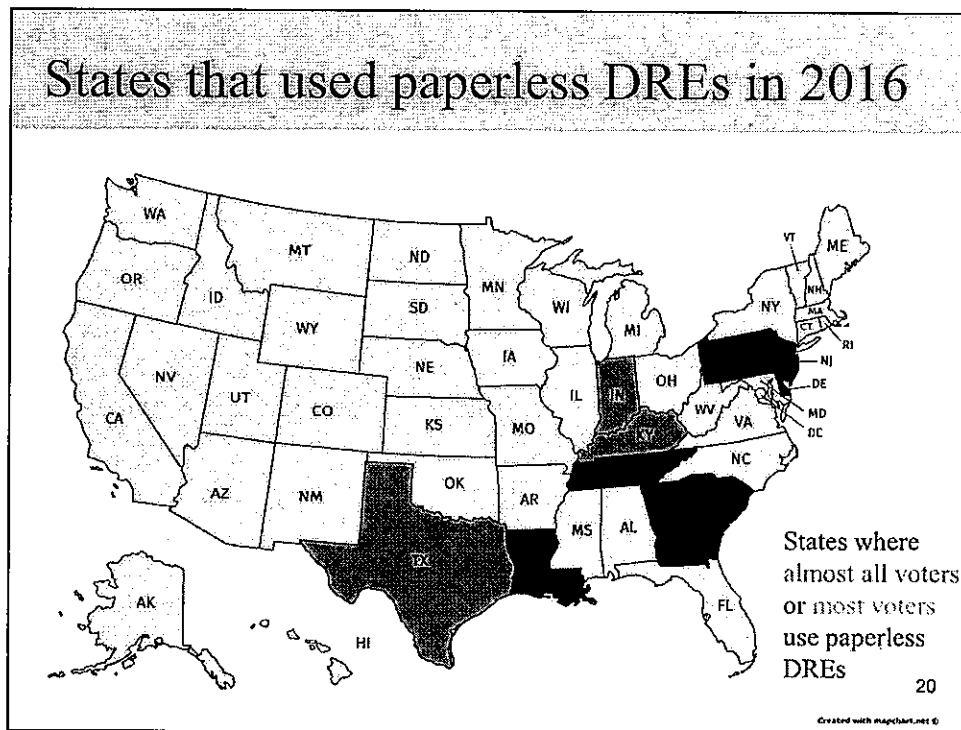
That way is: Voter-Verified Paper Ballots, counted by computer, audited by direct inspection (independent of hackable computers), of a statistically appropriate random sample.

27

What about a VVPB printer?

During 2004-2008, we thought that a "voter verified paper ballot" printer, attached to a direct-recording electronic (touchscreen) voting machine, was a good idea.
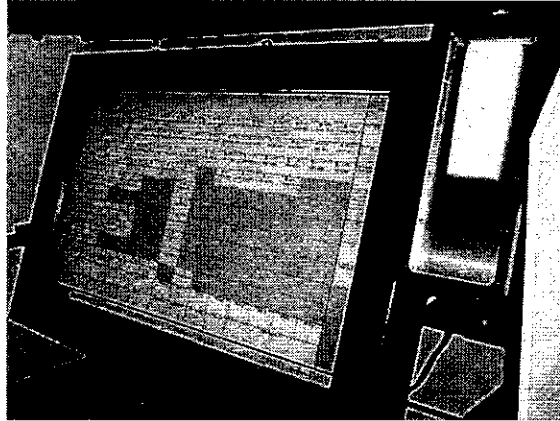
(This model is used in Warren County, New Jersey)

It's far better than a DRE *without* a VVPB, because the VVPBs are auditable and recountable; but the consensus now is that optical-scan is better. [28]

The reason is that most voters don't actually pay attention to the paper slip (shown here at upper right), so we can't be at all sure that what's marked on the paper corresponds to what the voter chose.

In contrast, if the voter marks an op-scan ballot with a pen, or carries the paper ballot from the BMD to the ballot scanner, then we have better assurance that the computer can't cheat in what it writes on the ballot.

29

New Jersey counties should adopt optical-scan voting

(It works well in at least 37 other states!)

Voter marks op-scan ballot

Voter feeds ballot to scanner

Paper ballot drops into ballot box

Rats!

Ballots can be recounted by hand

29

This is the standard method now in the United States.

Optical-scan can be used in NJ now
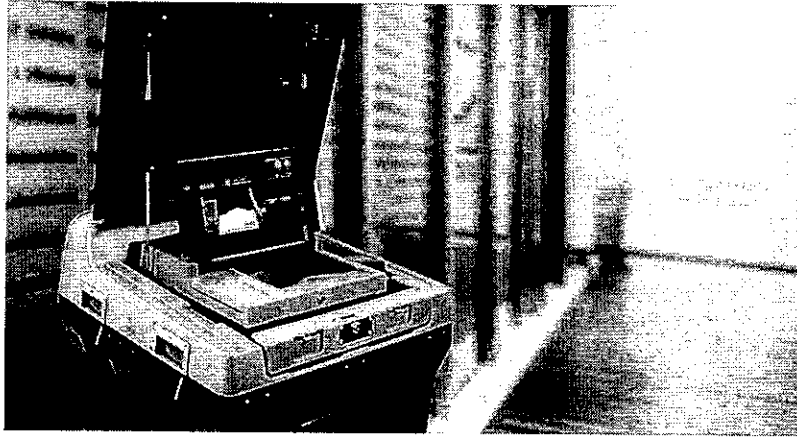
At least one optical-scan voting machine is certified (by the Secretary of State) for use in NJ: The ES&S model DS200.

30

This is not the only optical-scan voting machine that would be reasonable to purchase. It is not perfectly secure; no voting machine is! That's why we need audits. However, it's a competent machine; New York State switched to this machine in 2012 (from lever machines) without much fuss.

Ballot marking device (BMD)
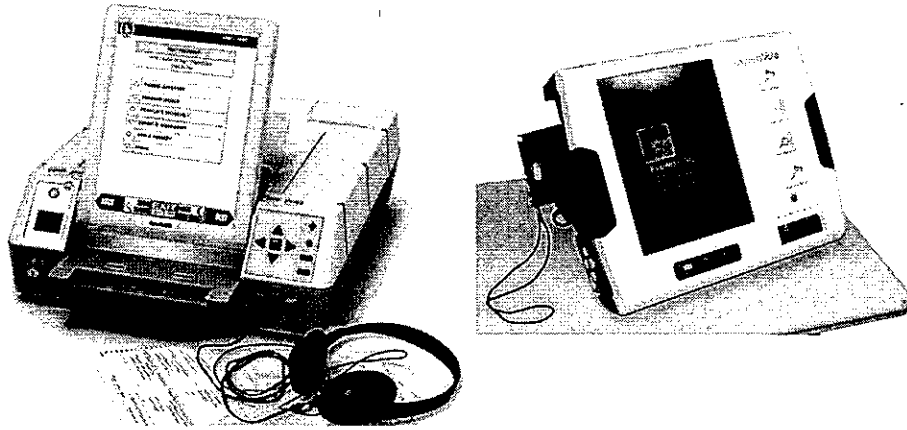
Need one of these in each polling place (not in each *precinct!)*,
to accommodate voters not able to mark an optical-scan ballot using a pen.   31

Available from several vendors

EAC certified BMDs, PCOS, and CCOS equipment

	Ballot Marking Device	Precinct OpScan	Central OpScan
ClearBallot	ClearAccess*	ClearCast*	ClearCount*
Dominion	ICX BMD	ICP	ICC
ES&S	ExpressVote 1.0	DS200	DS450,DS480
Hart	Verity TouchWriter	Verity Scan	Verity Central
Unisyn	OVI, FVT	OVO	OCS

*These systems are still in the EAC testing process as of October 2017

Source of information:
Brian J. Hancock, Director, Testing and Certification,
U.S. Election Assistance Commission

32

Cost

Major voting machine vendors don't advertise a "list price" (but estimate is $5000 per BMD or op-scan machine)

What you need:

In each *polling place* (not in each "election district" or "precinct", very often there are several precincts voting in the same polling place):

- One BMD
- One optical-scan voting machine

In each precinct:

Privacy booths (low tech) and/or tabletop screens for voters to mark their ballots by hand.

33

Testimony for the New Jersey State Assembly Judiciary Committee on A.4619, Oct. 26, 2017
Stephanie Harris - Chair of the Task Force on Voting Integrity, Coalition for Peace Action
Re: Support A4619 (S.3137) with Amendments

Once again I come before the Legislature to recount the sad tale of being disenfranchised by our voting technology. When I tried to cast my vote on a Sequoia Advantage machine in the 2004 Presidential Primary, the poll worker instructed me to press the cast vote button again as the vote was not registering. After three tries, he said he thought the vote was cast, but he was clearly not sure. After that I vowed to vote only on paper, so have been using vote by mail ballots. However, this July I received a letter that my vote in the gubernatorial primary had not been counted as it was found one month after the election in a pile of mail in the Hamilton, NJ Post Office. These incidents, combined with all of the news of election hacking in 2016 have led me to conclude that it is time for New Jersey to provide all voters with paper ballots that can be tabulated by optical scan machines.

In 2004 I became a plaintiff in the lawsuit of the Coalition for Peace Action requesting the Court to ban electronic direct recording electronic voting machines (DRE's). While the Court took 12 years to give a final judgment in the case, it had a profound influence on the Legislature, which in 2005 passed a bill requiring Voter Verified Paper Ballots, and in 2008 another bill requiring an audit. Unfortunately, both laws were not implemented due to a lack of funding. In 2005 the Legislators recommended a Voter Verified Paper Audit Trail (VVPAT), which was not yet a proven technology. The prototype of an add-on machine for the existing DRE's was rejected as too cumbersome and insecure. The current technology used in most states today is a precinct based optical scan machine that can tabulate the paper ballots voters have hand marked. While it is possible to corrupt the software of these machines, when coupled with a well-designed audit after the election, hacking can be detected. This system would ultimately save money for the State as fewer machines are needed than the current DRE's, thereby reducing the cost of purchase, storage, maintenance, transportation, and programming. There is already an optical scan machine certified in New Jersey (the ES&S D200), which is successfully used in New York and other states. So the only element lacking currently is the political will to replace our aging and insecure machines.

A.4619 is a small first step in this process. While the wording has to be changed to require a voter marked paper ballot (rather than the VVPAT in the original law), we support this important bill and praise its sponsors. We would prefer that the Legislature require a change to a paper ballot mandatory by a fixed date, and provide the Counties with the necessary funds. The Coalition for Peace Action has submitted amendments to A.4619 with three options: 1) change the wording in A.4619 to reflect the necessity of having a hand-marked paper ballot with the voter depositing it into an optical scan machine for tabulation; 2) change the wording in an appropriation bill, as proposed by Assemblyman Gusciora, that reflects the same change; 3) a mandatory statewide deployment of paper ballot voting systems as of a date certain with an appropriation. We support the use of hand marked paper ballots and optical scan machines, and a ballot marking device for the disabled as separate from a vote tabulator.

Elections are the foundation of our democracy, and the 2018 election will be one of the most consequential in recent history. The time to secure our right to having our votes counted as cast is now, the solution exists, and we hope that the Legislature will find the courage to address this pressing problem.

October 26th 2017

New Jeresy Legislature Assembly Judiciary Committee

Testimony in Support of Assembly Bill No. 4691 /⁹

Ann Rea

BlueWaveNJ

Electoral Reform Group Co-Leader

1 Shale Lane

Clifton NJ 07013

Area197@gmail.com

Last year, Donald Trump predicted that the election was likely to be rigged. That was a wild and unhelpful exaggeration. A majority of American polling places use transparent, common sense measures that make our elections trustworthy — features like paper ballots. The way to make our system better is not to panic about conspiracy theories, but rather to double down on the things we are already know work well, and adopt trusted voting procedures for every precinct in New Jersey.

States that keep the "faith based" DRE machines risk the consequence of contested elections. This example is from an August 24 2017 USA Today article regarding the June 2017 special election to fill Tom Price's House seat in Georgia:

> ... there is a .... special election suit [that] if successful, it would be what election experts believe is only the second time an election was overturned due to voting computer issues. The first such case came in 2011 in Fairfield Township, NJ., where a computer programming error gave votes for one set of candidates to their opponents. In that case a superior court judge ordered a new election.
>
> https://www.usatoday.com/story/tech/2017/08/24/election-hacking-lawsuit-over-heated-georgia-race-could-sign-whats-come/574313001/

It's not complicated- New Jersey's DRE voting machines do not instill confidence and cannot be checked. These machines have, and will, trigger costly law suits and do-over elections.
Our next voting machines must be more reliable, more usable, and can be less expensive than the current system. There is a possibility of using commercial-off-the-shelf hardware, such as printers and tablets, and adapt them for voting. This would be more cost effective, and provide an auditable voter marked paper record. Our state should prepare to vet new systems for secure voting and adopt one as soon as possible.

Right now, in Washington DC, there is a bi-partisan push to secure America's voting equipment. In fact, there is reason to hope that the federal government may step-up to the challenge and provide some much-needed funding for voting technology upgrades. Sens. Lindsey Graham (R-N.C.) and Amy Klobuchar (D-Minn.) co-sponsored an amendment to the National Defense Authorization Act that would provide grants to help states purchase new equipment. In the House, Rep. Mark Meadows (R-N.C.) and Jim Langevin (D-R.I.) co-sponsored a companion

to the Graham-Klobuchar amendment, called the Paper Act. Such bipartisan support for elections funding is a recognition of not only the scale of the problem but the potentially detrimental consequences of inaction.

https://www.brennancenter.org/blog/virginia-takes-steps-secure-election-infrastructure

When this bill, the National Defense Authorization Act, was voted on this September, the Senate added 37 Billion *more* for military spending than President Trump requested. Funds for upgrading the voting machines in New Jersey are vital to our national security and the funds are there. Not only do our citizens crave secure election but the strength of our military depends on the protection of our vote. US elections must be safe and secure so that in the event that the military is deployed, the citizens of New Jersey and the United States will have the utmost confidence that our leaders who take this most serious act, have been properly, provably, and fairly elected.

https://www.nytimes.com/2017/09/18/us/politics/senate-pentagon-spending-bill.html

Ann Rea 10/26/17 Testimony

Verifiedvoting.org
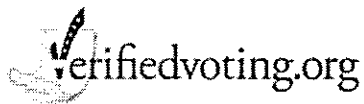
Testimony of Verified Voting
Contact: susan@verifiedvoting.org
917 796 8782

New Jersey State Assembly
Judiciary Committee
Re: A-4619 (S – 3137) - SUPPORT <u>WITH AMENDMENTS</u>

October 26, 2017

Thank you for the opportunity to submit testimony on A-4619.

Verified Voting is a national non-partisan, not for profit research and advocacy organization founded by computer scientists and committed to safeguarding democracy in the digital age. We promote technology and policies that ensure auditable, accessible and resilient voting for all eligible citizens. We urge you to <u>adopt the proposed amendments</u> and vote "YES" on A-4619.

New Jersey is one of only a handful of states whose voters are still casting votes on entirely electronic voting systems, direct recording electronic (DREs). Because these systems record votes directly onto computer memory without any independent paper record of the vote, they are especially vulnerable to <u>undetectable</u> and <u>uncorrectable</u> errors in the vote count.

Numerous studies and security evaluations of DRE systems over the years have found that the DREs in use in New Jersey have insecurities making them vulnerable to undetectable manipulation and tampering.[1] Because DRE systems prevent anyone from verifying that the electronic tally accurately reflects voter intent, many States have discontinued the use of electronic DRE voting systems in favor of paper ballots. In 2006 only 25% of voters nationwide cast their ballots on paper but in 2017 more than 70% of U.S. voters marked a paper ballot.[2]

In 2007 the California and Ohio Secretary of States conducted comprehensive security reviews of their systems.[3] The alarming security flaws and lack of auditability of the DRE devices led both states to discontinue use of paperless DREs and switch to voter-marked paper ballots and optical scan voting machines.

---

[1] Gross, Grant, "Security vendor demonstrates the hack of a U.S. voting machine," *PC World*, Nov. 7, 2016, "Hacking the AVC Advantage Voting Machine," http://www.cs.princeton.edu/~appel/voting/advantage-hacking.html
"Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage," Checkoway, Feldman, Kantor, Halderman, Felton, Shacham, https://cseweb.ucsd.edu/~hovav/dist/avc.pdf

[2] https://www.verifiedvoting.org/verifier/

[3] California Secretary of State "Top-to-Bottom Review," http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/
Ohio Secretary of State Jennifer Brunner, "Project EVEREST, Evaluation and Validation of Election Related Equipment Standards and Testing," https://votingmachines.procon.org/sourcefiles/Everest.pdf

1

Optical scan voting systems in which a voter records her vote on a paper ballot provide resilience against tampering, that is, the paper record allows jurisdictions to check the electronic tally against the paper ballots and detect any discrepancies. DREs, by design, are unable to provide this assurance. The paper ballot provides a permanent, physical record of voter intent that cannot be altered by a cyber attack and is available for use in a post-election audit to confirm the election tally is correct. In 2011 the U.S. Election Assistance Commission directed the National Institute of Standards and Technology (NIST) to provide guidance on how to audit a DRE voting system to confirm the vote tallies are correct or to catch any potential error or tampering. NIST convened an Auditability Working Group to study the question. **The NIST Auditability Working Group found that any system that does not provide a voter-verified paper record of voter intent will be susceptible to undetectable errors in the vote count.[4] Put simply, it is impossible to know for sure that the vote tallies generated from DRE voting machines are correct.**

The studies cited above have mostly been conducted over a decade ago, when the cyber threat to elections was more theoretical than actual, however those days are over. We are in a new paradigm; in the last year the U.S. Intelligence Community has warned us that foreign adversaries have been probing our election infrastructure, looking for weaknesses.[5] In a March hearing before the U.S. House Intelligence Committee, the former director of the FBI testified ominously that "[t]hey'll be back."[6] We must face the chilling reality that our enemies have the will, intention and ability to tamper with our election infrastructure, potentially delegitimizing our elections and destabilizing our government. This is a national security issue. The legislature has the opportunity to act now, to safeguard New Jersey's elections and remove the insecure, untrustworthy DREs in use and replace them with voter-marked paper ballots.

The broadly accepted evidence that paperless DREs are insecure and untrustworthy drove the legislature to pass a measure to require voter-verified paper records in 2005 but it failed to fund and implement this law. For over a decade, New Jersey voters have continued to use an untrustworthy and unreliable voting system. Given the recent revelations of nation-state adversaries, the urgency of replacing unverifiable voting systems with new systems is more pressing than ever. New Jersey must replace its outdated and unverifiable voting equipment.

Threats to our election systems demand action

In response to the threat of election interference – and because, like New Jersey, it will be conducting several significant state-wide races this November – the Commonwealth of Virginia ordered a security review of its paperless DRE voting systems including the AVC Advantage and the Sequoia AVC Edge[7] (machines that count the overwhelming majority of votes in New Jersey). As a result of this review, the Virginia Commissioner of

---

[4] Report of the Auditability Working Group, Jan. 14, 2011, U.S. Election Assistance Commission
https://www.eac.gov/assets/1/28/AuditabilityReport_final_January_2011.pdf

[5] Isikoff, Michael, "FBI says foreign hackers penetrated state election systems," *Yahoo News,* Aug. 29, 2016

[6] Washington Post Staff, "Full Transcript: FBI Director James Comey testifies on Russian interference in 2016 election," March 20, 2017

[7] https://www.elections.virginia.gov/Files/Media/Agendas/2017/DREdecertificationmemofinal09-08-17.pdf

42x

Elections recommended the immediate decertification of all DREs in the Commonwealth. Virginia's bipartisan State Board of Elections voted unanimously to decertify all the DREs before the November elections. In its decertification resolution, the Board stated, "the DRE devices analyzed all exhibited a range of demonstrated, documented, or potential vulnerabilities that materially impact the integrity of the voting process, availability of the voting systems, or integrity of election results."[8] Though regrettably it's too late for New Jersey to take action before the November 2017 elections, we strongly urge the legislature to pass A-4619 with proposed amendments.

In April the Coalition for Peace Action submitted proposed changes to A-4619 to Assemblywoman Muoio that would amend A-4619 from requiring all voting systems "produce a paper record of each vote cast" to require "a voter-marked paper ballot for every vote cast in the State," and that all new voting systems purchased or leased "be paper ballot voting systems comprising one automatic ballot tabulator per election district for the tabulation of such voter-marked paper ballots, and one accessible non-tabulating ballot marking device per election district to assist voters with disabilities and others needing assistance in marking paper ballots. All voter-marked paper ballots may be tabulated by automatic ballot tabulator or by hand."

It is critical the legislature adopt these amendments. In 2005, when New Jersey passed its law to require a voter verified paper ballot, less was known about the cost, efficacy, and auditability of DREs equipped with voter-verified paper record. Over a decade later we know these systems are more costly, inefficient and difficult to recount or audit than a voter-marked paper ballot scanned by a ballot tabulation device. States are moving away from such systems in favor of voter-marked paper ballots. In this instance, New Jersey's slow action provides a benefit – the legislature can avoid the mistake and extra expense of purchasing DREs that produce a voter-verified paper record.

We strenuously urge the legislature to adopt the amendments proposed by Verified Voting and the Coalition for Peace Action and vote YES on A-4619.

---

[8] https://www.elections.virginia.gov/Files/Media/Agendas/2017/DREdecertificationmemofinal09-08-17.pdf

43

Ballot Marking Devices Must be Non-tabulating

Ballot marking devices must be non-tabulating for several reasons, including increased security, increased voter privacy, and decreased costs per polling place.

Security Concerns

Security, integrity and accuracy concerns are caused when all of the software relevant to a voting system is included in one machine, as would be the case with a ballot marking device that also tabulates votes. Some of the software would enable the voter to mark the ballot, some would enable the machine to record votes digitally, and some would tabulate the digitally recorded votes. If all of that software is included in the same machine, there is a possibility that some of it (or other programs in the machine) could inadvertently or as a result of intentional malfeasance impact those programs in a way that would alter the intentions of the voters and or the accuracy of the tallies. An audit of the electronic tallies might indicate if that happened, although an audit is only as effective as the audit records used to check the electronic tallies.

The security problems described above are exacerbated if and when a substantial portion of voters who use the system do not review their printed ballots before depositing them in a scanner. Even if a ballot marking device prints a ballot for every vote cast, and even if the voters must deposit those ballots into a separate scanner, if any substantial portion of the voters using the system do not review their ballots, the value of the ballots as an audit tool is diminished in equal proportion. This is one of the primary problems with DREs that produce voter verified paper records; voters don't necessarily review them. Other problems with VVPATs are described in the attached summary.

These security problems would also be virtually unresolvable if and when the ballot marking device and the scanner are the same machine, and that machine is used by all voters; ballots would likely go from the "printer" directly into the ballot box and voters would not necessarily even have an opportunity to review them before that happens. That would make the ballots worthless as audit records.

Voter Privacy Concerns

Most ballot marking devices are currently used only or primarily to enable voters with disabilities to mark ballots privately and independently, as required by federal law. If the ballot marking devices also tabulated the votes on those ballots, the privacy of disabled voters as a group would be violated because how they voted as a group would be obvious as soon as the votes were tabulated.

Allowing or requiring all voters to vote on ballot marking devices would address that concern, although it would at the same time create the security concerns described above.

When all voters create voter-marked paper ballots, either by marking them by hand or by marking them through the use of a non-tabulating ballot marking device, then all ballots

44x

of all voters can be read by one scanner, and the privacy of all voters is protected because only one tally is produced. This prevents privacy violations, while also minimizing the security concerns described above and the cost concerns described in the following paragraphs.

Cost Concerns

Federal law currently requires at least one accessible voting system per polling place. Jurisdictions that have deployed optical scan voting systems as the standard voting system in each polling place have deployed either a ballot marking device or a direct recording electronic (DRE) voting machine to meet their disability access requirements in each polling place. Either way, each polling place only requires one optical scanner and one accessible voting machine. DREs without VVPATs are unacceptable for security reasons, and are already illegal pursuant to New Jersey's (albeit funding contingent) paper record requirement. DREs with VVPATs have the security problems described above and also currently provide no way for disabled voters to review their VVPATs. Therefore, non-tabulating ballot marking devices must be used for disability access.

However, if all voters were required to vote on the ballot marking device originally deployed in order to meet disability access requirements, then many more machines would be required for every polling place than would be required if the ballot marking devices are only used for disability access and all other voters marked their ballots by hand. For example, although there is some ambiguity in the statutory definitions, New Jersey requires either 4 electronic voting devices for every 750 voters (19:4-11), 5 electronic voting devices for every 1,000 voters (19:4-12) or 8 electronic voting devices for every 1,500 voters (19:4-12). In other words, depending on the number of voters allocated to a polling place, approximately one electronic voting device (19:53A-1 defines a "voting device" as "an apparatus which the voter uses to record his votes on a tabulating card") is required for every 200 voters at the most. If the voting machines are not accessible, an accessible one would be required in addition at each polling place.

However, if most voters mark their ballots by hand, then only one electronic voting device would be required at each polling place, accompanied by one automatic ballot tabulator. This would not prevent jurisdictions from deploying more ballot marking devices if they chose to. It would simply make it clear that they would not be required to. If a jurisdiction deploys enough ballot marking devices for all voters, however, voters who wish to mark their ballots by hand must still be allowed to do so.

Paper Ballots are Superior to Voter Verified Paper Records

"Currently, aside from the handful of jurisdictions that still use punch cards, there are only two forms of . . . independent [paper] records, One is paper ballots, which are filled out by the voter ("voter-marked") either manually or through the use of an assistive interface known as a ballot marking device, and can be tallied by a scanner or counted by hand. The other is VVPATs, which are contemporaneously printed by DRE voting machines. Sighted voters who use DRE voting machines with paper trails have the opportunity to review a paper record of their vote before casting it.

All three organizations involved in writing this report support the use of voter-marked paper ballots, which are made accessible through the use of ballot marking devices; there are currently no VVPATs that are accessible to the visually impaired, and the authors have other concerns about them set forth below. Voter-marked paper ballots and VVPATs should be treated as the vote of record in all counts, audits and recounts. If and to the extent that the paper ballots or records are lost, damaged or otherwise compromised, that must be addressed. For example, if the number of compromised paper ballots or records exceeds the margin of victory, a new election should be held.

Paper ballots with ballot marking devices for accessibility offer superior records for the following reasons:

Paper ballots are superior to VVPATs as audit and recount records While no voting system is perfect, the authors believe that paper ballots and optical scan systems, used with an accessible ballot-marking system, offer significant advantages over VVPAT-equipped DRE systems. Optical scanners are more reliable and auditable, and are easier for poll workers and for voters who do not need assistance to mark a paper ballot to use. Most importantly, when a voter marks his or her own ballot, it is automatically a "voter-verified" record of the vote. In contrast, if the DRE prints a VVPAT, it only becomes "voter verified" if the voter bothers to check it or, as would not be the case for a visually impaired voter, is even able to check it. The only way a visually–impaired voter can currently verify a paper copy of the ballot through the use of technology, which allows the voter to vote independently, is by using an accessible ballot marking device to mark the ballot that also enables audio read-back of the voter's choices from the printed or marked ballot.

VVPATs are very small, are viewable through a small window on the voting machine, and the font in which they are printed is also very small. This makes them much harder to read than a full size ballot, decreasing the likelihood that all voters will confirm them. That compromises the value of VVPATs as audit records as compared to voter-marked paper ballots. In addition, paper ballots must be sturdy enough to be fed through a

---

scanner and are therefore generally more durable than, for example, standard copier paper. That makes them easy to handle and unlikely to be damaged during even multiple hand-counted audits and recounts. In contrast, the VVPATs currently in use are less durable than standard copier paper, more fragile, subject to loss of data if exposed to heat, and more difficult to handle during a hand-count audit, because they are generally printed on thin paper similar to that used to print receipts from ATMs or cash registers. This further compromises their value as audit records as compared to voter-marked paper ballots.

Optical scan systems do not present the disenfranchisement risk DREs present in the event of machine failure When optical scanners are used in the precinct as the standard polling place equipment, voters who do not need assistance to mark a paper ballot can continue voting uninterrupted regardless of machine failure. Although any over-vote notification feature provided by the scanner would not be available, and over-vote notification is a requirement if the Help America Vote Act, such voters can still mark their ballots without waiting and deposit them in an auxiliary bin. The ballots can be counted later by machine or by hand. The failure of the optical scanner itself also would not impact voters who do need assistance because they would be voting on a DRE or ballot marking device. In contrast, when VVPAT-equipped DREs are used, when the DRE fails, both the DRE and its VVPAT printer are useless. Voting by those who do not need assistance cannot continue unless and until emergency paper ballots are deployed. With respect to voters who do need assistance to mark a ballot, the failure of the accessible voting equipment (whether DRE or ballot marking device) would result in a violation of the right to vote privately and independently under the Help America Vote Act, and those voters also would not be able to continue voting unless and until paper ballots and assistance in marking them are provided.

Many DREs are required to serve the same number of voters that can be served by just one optical scanner With respect to voters who can mark their ballots without assistance, generally, only one optical scanner is needed to process thousands of voters. This is because those voters mark their ballots at ballot marking tables, and only occupy the scanner for the one or two seconds it takes to feed the ballot into it. In contrast, one DRE or ballot marking device can only efficiently handle about 200 voters before lines form.

This is because voters (whether they require the machine for access or are using it as the standard polling place equipment) occupy the DRE or ballot marking device for the entire time it takes to cast the ballot. That is, they are registering their choices on the machine itself, like a bank ATM. The cost of providing one accessible piece of voting equipment per precinct, as required by law, is essentially the same for optical scan and DRE precincts.

VVPATs are not accessible audit records, while paper ballots marked by accessible ballot marking devices are With a VVPAT-equipped DRE, only the DRE itself is accessible to disabled voters. Currently used VVPAT systems do not provide audio-read-

47v

back of the printed record for voters with limited or no vision. The only way a voter who needs assistance can currently verify a paper copy of the ballot through the use of technology, which allows the voter to vote independently, is by using an accessible ballot marking device to mark the ballot that also enables audio read-back of the voter's choices from the printed or marked ballot.

For all of these reasons, the authors believe that paper ballots and optical scan systems, accompanied by accessible ballot marking devices, should replace DREs (with or without VVPAT printers). All three organizations also agree that if and to the extent that DRE systems remain in use, they should not be used without (1) a VVPAT printer; (2) guidance to ensure that voters check the paper records for accuracy when voting; and (3) sufficient emergency paper ballots on hand in case of machine failures or malfunctions."

DRE BAN (FUTURE PURCHASES)

SYNOPSIS

Requires a voter-marked paper ballot for every vote cast in the State, and requires any new voting machines purchased or leased for use in any elections in this State to be paper ballot voting systems comprising one automatic ballot tabulator per election district for the tabulation of such voter-marked paper ballots, and one accessible non-tabulating ballot marking device per election district to assist voters with disabilities and others needing assistance in marking paper ballots. All voter-marked paper ballots may be tabulated by automatic ballot tabulator or by hand.
~~to produce paper record of each vote cast~~.

CURRENT VERSION OF TEXT

As introduced.

An Act concerning the requirement for a voter-marked paper ballot for every vote cast in the state and paper ballot voting systems to tabulate them ~~voting machines to produce a paper record of each vote cast~~ and amending R.S.19:48-1 and P.L.1973, c.82.

Be It Enacted *by the Senate and General Assembly of the State of New Jersey:*

1. R.S.19:48-1 is amended to read as follows:

19:48-1. a. Any thoroughly tested and reliable paper ballot voting ~~machines~~ system may be adopted, rented, purchased or used, which shall be so constructed as to fulfill the following requirements:

(a) It shall secure to the voter secrecy in the act of voting;

(b) It shall provide facilities for such number of office columns, not less than 40 and not exceeding 60, as the purchasing authorities may specify and of as many political parties or organizations, not exceeding nine, as may make nominations, and for or against as many questions, not exceeding 30, as submitted;

(c) It shall, except at primary elections, permit the voter to vote for all the candidates of one party or in part for the candidates of one party or one or more parties;

(d) It shall permit the voter to vote for as many persons for an office as he is lawfully entitled to vote for, but no more;

(e) It shall prevent the voter from voting for the same person more than once for the same office;

(f) It shall permit the voter to vote for or against any question he may have the right to vote on, but no other;

(g) It shall for use in primary elections be so equipped that the election officials can stop a voter from voting for all candidates except those of the voter's party;

(h) It shall correctly register or record and accurately count all votes cast for any and all persons, and for or against any and all questions;

(i) It shall be provided with a "protective counter" or "protective device" whereby any operation of the machine before or after the election will be detected;

(j) It shall be so equipped with such protective devices as shall prevent the operation of the machine after the polls are closed;

(k) It shall be provided with a counter which shall show at all times during an election how many persons have voted;

(l) It shall be provided with a model, illustrating the manner of voting on the machine, suitable for the instruction of voters;

(m) It must permit a voter to vote for any person for any office, except delegates and alternates to national party conventions, whether or not nominated as a candidate by any party or organization by providing an opportunity to indicate such names or name;

(n) It shall be equipped with a permanently affixed box or container of sufficient strength, size and security to hold all voter-marked paper ballots and all emergency ballots and pre-punched single-hole envelopes and with a clipboard and a table-top privacy screen;

(o) It shall not use mechanical lever machines or punch cards to record votes.

(p) All voting booths or machines used in any election, whether used by voters to mark paper ballots by hand or by voters with disabilities or others needing assistance to mark a paper ballot with the assistance of a ballot marking device, –shall be provided with a screen, hood or curtain, which shall be so made and adjusted as to conceal the voter and his action while in the process of marking his or her paper ballotvoting.

(q) All ballot marking devices shall enable voters with disabilities and others needing assistance to mark a ballot to mark their ballots privately and independently, and shall be supplied with privacy sleeves to ensure that the voted ballots will be transported to the automatic ballot tabulator without violating the privacy of the voter's vote selections;

(r) Ballot marking devices shall not tabulate votes;

(s) All automatic ballot tabulators shall provide a mechanism that examines a ballot card for overvotes, stray marks and other irregularities and returns it to the voter for correction of the error at the polling place before it is cast and tabulated; and

(t) All automatic ballot tabulators shall permit a voter to twice receive a replacement ballot card if the voter wishes to change any vote or in the event that the original ballot card or the next subsequent ballot card is defective, spoiled or otherwise incapable of recording the intended vote of the voter.

It shall also be provided with one device for each party for voting for all the presidential electors of that party by one operation, and a ballot therefor containing only the words "presidential electors for," preceded by the name of that party and followed by the names of the candidates thereof for the offices of President and Vice-President and a registering device therefor which shall register the vote cast for such electors when thus voted collectively.

b. (1) By January 1, 2009, each voting machine shall produce an individual permanent paper record for each vote cast, which shall be made available for inspection and verification by the voter at the time the vote is cast, and preserved for

later use in any manual audit. In the event of a recount of the results of an election, the voter-verified paper record shall be the official tally in that election. [A waiver of the provisions of this paragraph shall be granted by the Secretary of State if the technology to produce a permanent voter-verified paper record for each vote cast is not commercially available.]

(2) The provisions of paragraph (1) of this subsection shall be suspended until: (i) the Secretary of State and the State Treasurer certify in writing that sufficient funds have been provided by the federal government and received by the State to offset the entire cost of ensuring that each voting machine used in this State produces an individual permanent paper record for each vote cast; or (ii) the annual appropriation act contains an appropriation of sufficient funds to ensure that each voting machine used in this State produces an individual permanent paper record for each vote cast and such appropriated funds have not been reserved by the Governor under a spending reduction plan; or (iii) the Secretary of State and the State Treasurer certify in writing that sufficient funds have been provided by the federal government and received by the State, and the annual appropriation act contains an appropriation of sufficient unreserved funds, to ensure, when such funds are combined, that each voting machine used in this State produces an individual paper record for each vote cast.

c.   Each voting ~~machine~~ system newly-purchased or leased following the effective date of P.L.   , c.   (pending before the Legislature as this bill) shall require the use of a voter-marked paper ballot for every vote cast, and shall be a paper ballot voting system comprising one automatic ballot tabulator and one accessible ballot marking device to assist voters with disabilities and others needing assistance in marking paper ballots. All voter-marked paper ballots may be tabulated by such automatic ballot tabulators or by hand. All such voter-marked paper ballots shall be ~~produce an individual permanent paper record for each vote cast, which shall be made available for inspection and verification by the voter at the time the vote is cast, and~~ preserved for later use in any manual audit or recount. In the event of an audit or recount of the results of an election, the tally of the votes on the voter-~~verified paper record of each machine~~marked paper ballots required under this subsection shall be the official tally ~~be used in the calculation of the official tally~~ in that election.
(cf: P.L.2009, c.17, s.1)

2.   Section 3 of P.L.1973, c.82 (C.19:53A-3) is amended to read as follows:
3.   Every electronic voting system, consisting of a voting device in combination with automatic tabulating equipment, acquired or used in accordance with this act, shall:
a.   Provide for voting in secrecy, privately and independently, except in the case of voters who have ~~received~~ chosen to receive assistance as provided by law;
b.   Permit each voter to vote at any election for all persons and offices for whom and for which he is lawfully entitled to vote; to vote for or against any question upon which he is entitled to vote; and the automatic ~~tabulating equipment~~ballot tabulator shall reject choices recorded on his ballot if the number of choices exceeds the number which he is entitled to vote for the office or on the measure;
c.   Permit each voter, at presidential elections, by one mark to vote for the candidates of that party for president, vice president, and their presidential electors;
d.   Permit each voter, at other than primary elections, to vote for the nominees of one

or more parties and for independent candidates; and personal choice or write-in candidates;

e.   Permit each voter in primary elections to vote for candidates in the party primary in which he is qualified to vote, and the automatic ~~tabulating equipment~~ballot tabulator shall reject any votes cast for candidates of another party;

f.   Prevent the voter from voting for the same person more than once for the same office;

g.   Be suitably designed for the purpose used, of durable construction, and may be used safely, efficiently, and accurately in the conduct of elections and counting ballots;

h.   When properly operated, record correctly and count accurately every vote cast, including all overvotes or undervotes and all affirmative votes or negative votes on all public questions or referenda;

i.   (1) By January 1, 2009, each voting machine shall produce an individual permanent paper record for each vote cast, which shall be made available for inspection and verification by the voter at the time the vote is cast, and preserved for later use in any manual audit. In the event of a recount of the results of an election, the voter-verified paper record shall be the official tally in that election. [A waiver of the provisions of this subsection shall be granted by the Secretary of State if the technology to produce a permanent voter-verified paper record for each vote cast is not commercially available.]

(2) The provisions of paragraph (1) of this subsection shall be suspended until: (i) the Secretary of State and the State Treasurer certify in writing that sufficient funds have been provided by the federal government and received by the State to offset the entire cost of ensuring that each voting machine used in this State produces an individual permanent paper record for each vote cast; or (ii) the annual appropriation act contains an appropriation of sufficient funds to ensure that each voting machine used in this State produces an individual permanent paper record for each vote cast and such appropriated funds have not been reserved by the Governor under a spending reduction plan; or (iii) the Secretary of State and the State Treasurer certify in writing that sufficient funds have been provided by the federal government and received by the State, and the annual appropriation act contains an appropriation of sufficient unreserved funds, to ensure, when such funds are combined, that each voting machine used in this State produces an individual paper record for each vote cast.

j.   Each voting ~~machine~~ system newly-purchased or leased following the effective date of P.L.   , c.   (pending before the Legislature as this bill) shall require the use of a voter-marked paper ballot for every vote cast, and shall be a paper ballot voting system comprising one automatic ballot tabulator and one accessible ballot marking device to assist voters with disabilities and others needing assistance in marking paper ballots. All voter-marked paper ballots may be tabulated by such automatic ballot tabulators or by hand. All such voter-marked paper ballots shall be ~~produce an individual permanent paper record for each vote cast, which shall be made available for inspection and verification by the voter at the time the vote is cast, and~~ preserved for later use in any manual audit or recount. In the event of an audit or recount of the results of an election, the tally of the votes on the voter-marked paper ballots ~~verified paper record of each machine~~ required under this subsection shall be

~~used in the calculation of~~ the official tally in that election.
(cf: P.L.2009, c.17, s.2)

3. This act shall take effect ~~on January 1 next following enactment~~immediately.

STATEMENT

Under current law, the requirement for the purchase of new voting machines or retrofitting of existing voting machines to produce a paper record of the votes cast has been suspended until funding is made available from State or federal sources. This bill would require that new voting ~~machines~~ systems purchased or leased following the bill's effective date must ~~produce a paper record of each vote cast~~satisfy the State's existing requirement for voter-verified paper records by requiring a voter-marked paper ballot for every vote cast, and the deployment of one automatic ballot tabulator and one accessible non-tabulating ballot marking device in each election district.

Specifically, the bill provides that each voting machine that is purchased or leased following the bill's effective date would be required ~~to~~ to be a paper ballot voting system, requiring a voter-marked paper ballot for every vote cast, and comprising one automatic ballot tabulator that shall tabulate such voter-marked paper ballots, and one accessible non-tabulating ballot marking device that shall assist voters with disabilities and others needing assistance in marking paper ballots that may then be tabulated by such automatic ballot tabulator. All of such voter-marked ballots shall be ~~produce an individual permanent~~ paper record ~~for each vote cast, which must be made available for inspection and verification by the voter at the time the vote is cast, and~~preserved for later use in any manual audit or recount. In the event of an audit or recount of the results of an election, the tally of the votes on the voter-marked paper ballots ~~verified paper record of each machine so purchased or leased~~would be ~~used in the calculation of~~the official tally in that election.

The bill also deletes a provision in current law that allows the Secretary of State to grant a waiver from the requirement to purchase new voting machines or retrofit all existing voting machines if the technology to produce a permanent voter-verified paper record for each vote cast is not commercially available. This change is intended to reflect that ~~the technology is now commercially available~~voter-marked paper ballots tabulated by automatic ballot tabulators are a vastly preferable, much more durable and otherwise superior method for satisfying the State's existing requirement for voter-verified paper records.

This bill is prospective in application, and would apply to paper ballot voting ~~machines~~systems purchased or leased following its effective date. The bill would take effect ~~on January 1 next~~immediately following enactment.

52

Voting machine bill

julie lips [jjlips@optonline.net]
Sent:Friday, October 20, 2017 3:17 PM
To: OLSaideAJU

I am writing in support of the Voting Machine Paper Trail Bill. Our elections have been compromised and we are due every security measure available. This bill is a start. I believe the next step should be to replace existing machines that do not have paper trail capability with those that do.

Julie Lips
973-615-6607

54 x

CHRIS CHRISTIE
Governor

LT. GOVERNOR KIM GUADAGNO
Secretary of State

October 25, 2017

Hon. John F. McKeon, Chair
Assembly Judiciary Committee
State House Annex
P.O. Box 068
Trenton, NJ 08625-0068

Dear Chairman McKeon:

Thank you for the opportunity to provide information to the Assembly Judiciary Committee regarding the security of New Jersey's voting machines. Please accept this letter that addresses several aspects of voting machine security.

The State's Voting Machines Are Accurate and Reliable.

The Division of Elections is committed to ensuring the integrity of the State's elections. Voting machines play a critical role in this process as they are the means by which votes are recorded and tabulated. There are approximately 11,000 voting machines presently in use Statewide; AVC Advantage machines are the vast majority of the voting machines used in the State as they are used in 18 of the State's 21 counties. The AVC Advantage is a full-face direct recording electronic voting system: voters make their choices directly on-screen, and votes are recorded internally to RAM. Notably, AVC Advantage machines are not connected to the Internet and thus are not vulnerable to online hacking activity.

The accuracy and reliability of the AVC Advantage voting machine were challenged in a lawsuit that went to trial in Superior Court in 2009. In resolving that case, the court held that "[t]he record is void of any evidence to establish that any election has ever been compromised due to the fraudulent manipulation of an AVC voting system." Gusciora v. Corzine, 2010 N.J. Super. Unpub. LEXIS 2319, at *289 (Law Div. Feb. 1, 2010).[1] The Court further found "no evidence that the AVC, in its normal state: (1) has design flaws that cause votes to be lost; (2) encourages voter and poll worker error; or (3) permits fraudulent manipulation." Id. at *293.[2] These findings were not disturbed on appeal. See Gusciora v. Christie, 2013 N.J. Super. Unpub. LEXIS 2278 (App. Div. Sept. 16, 2013).

---

[1] Moreover, according to the Court, "[t]here has never been a demonstrated incident of an attempted attack or a verified attack of any AVC voting system in the United States since its use began at least as early as 1979," and "[n]o AVC has ever been demonstrated to have been hacked, other than in an academic setting, in this State or any other State." Id. at *290.

[2] That is at least in part because "[t]he technical barriers to producing fraudulent firmware, and the necessary step of reverse engineering the source code, are substantial" and, further, because "[t]he notion that fraudulent firmware can continue to operate, as anticipated, for future elections, is completely unrealistic." Id. at *291.

1

A Recently Developed Seal-Use Protocol Has Strengthened Voting Machine Security.

Following the conclusion of the aforementioned case, and consistent with the Court's directive, the Division of Elections implemented a protocol for placing tamper-evident seals on all voting machines in an effort to further enhance their security and protect against intruders. Again, since our machines are not connected to the Internet, the physical security of the machines and their ports are paramount in ensuring security. The seals, which cover exposed ports and other access areas on the voting machine, including, for instance, the port where the results cartridge resides, must meet certain standards. Also per the protocol, training as to the proper installation and inspection of seals must be provided, seal inspections must be performed and recorded before and after every election, and those who work on voting machines must pass a criminal background check. This Statewide seal-use protocol is yet one more way in which the security of the State's voting machines has been strengthened.

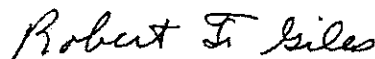## Strong Partnerships with State and Federal Agencies Aid Response to Emerging Threats.

Recognizing that election systems are part of the nation's critical infrastructure, the Division of Elections is collaborating with the New Jersey Office of Homeland Security and Preparedness, the United States Department of Homeland Security (DHS), and the Federal Bureau of Investigation to assess and devise additional safeguards to secure the integrity of the State's voting apparatus. Notably, New Jersey is one of seven states participating in a pilot project with the Multi-State Information Sharing Analysis Center, a DHS affiliate, to develop best practices for sharing election threat information around the country. By facilitating the sharing of information, these partnerships enable the Division of Elections to stay attuned to, and better respond to, emerging threats to voting processes.

Assembly Bill No. 4619.

Assembly Bill No. 4619 addresses the ongoing debate over the need for a voter-verified paper recording of votes and requires all future voting machines that are purchased or leased to produce an individual permanent paper record for each vote cast. For your information, machines capable of producing paper recordings tend to range in price from $5,000 to $7,000 per unit. Thus, the cost to replace, on a go-forward basis, the approximately 11,000 voting machines currently in use could exceed $75 million.

Thank you again for the opportunity to present this information to the Assembly Judiciary Committee.

Respectfully submitted,

Robert F. Giles

Robert F. Giles
Director, Division of Elections

2

56

Testimony of Charles P. Lamb to the New Jersey Assembly Judiciary Committee on bill A4619

October 26th, 2017

Introduction

I am in favor of eliminating further delay in the implementation of voter-verified paper records however I believe some remedial action is required before this should be done. The intent of the legislature has been mis-interpreted in the requirements established by the Attorney General and applied by the Voting Media Examination Committee to the detriment of the voting process. Below I have described three cases where the implementation of the legislation requires correction.

All of the information on which my opinion is based has been obtained from the World Wide Web. Additional information would be helpful but I have not had the time to obtain it through requests made to the voting machine vendors or OPRA requests to the various state entities.

Non-standard abbreviations used in this document

VMEC – Voting Media Examination Committee

VVPRC – Criteria for Voter-Verified Paper Record for Direct Recording Electronic Voting Machines

"Quick-Pick" voting

Problem – VVPRC IV.C.5 requires the machine to operate so that the voter is allowed no more than three attempts to produce a paper record indicating the voter's selections. On the third attempt the selections indicated on the paper record must be cast regardless of whether or not the voter approves of the selections printed thereon. The requirement that a ballot be cast which is not approved by a voter is repugnant to the concept of a democratic republican government and a violation of the New Jersey and Federal Constitutions.

Proposed Remedy – If more than a set number of machine printed paper records is rejected by the voter the machine should disable itself for that voter, print a paper record indicating so, and not cast any ballot for that voter. The voter should then be permitted to vote using a Provisional Ballot.

Discussion – The reason a paper record of each vote is being required by the legislature is that the legislature recognizes that a voting machine may on occasion operate contrary to design. However, the requirement that the voter only be permitted three attempts before being forced to vote implies that the machine is operating correctly and that the failure to produce an acceptable printed paper ballot can only be due to an error of the voter. This requirement was questioned more than once by members of the VMEC but members were informed that this requirement was mandated by New Jersey law. The specific law requiring this was not mentioned. My best guess is that the law being referred to is N.J.S.A. 19:15-29. Although the legislature in N.J.S.A. 19:53A-13 states that the provisions of Title 19 are applicable to electronic voting systems I believe this particular part was intended by the legislature to only apply to manually marked ballots—not voter-verified paper records.

Paper record type size

Problem – VVPRC III.A.4 specifies the type font size on the paper record as being in the ranges 3.0-4.0 mm and 6.3-9.0 mm as may be selected by the voter or poll worker. This size may be achieved by magnification of the paper record. Allowing this size to be achieved by magnification is not acceptable. No specification is made as to the color of the lettering and the style of the type. This should be done to ensure that the voter-verified paper record is readable.

Proposed Remedy – The type used on the paper record should meet the requirements for size, style, and color as prescribed by the legislature in N.J.S.A. 19:14-16 for manually marked paper ballots and in N.J.S.A. 19:49-2 for voting machines without the use of magnification. The legislature should modify the requirements of N.J.S.A. 19:49-2 so that the paper record need not have the prescribed arrangement and shall use black ink for public questions.

Discussion – The voter-verified paper record should meet the same requirements for legibility as a manually marked paper ballot and the same requirements as the ballot displayed on the voting machine because it serves the same function to the voter. N.J.S.A. 19:14-16 specifies candidate name and title to be in 10 point type [3.51mm]. A voter capable of reading a machine or paper ballot should be capable of reading the voter-verified paper record in order to determine that the choices printed thereon are correct. Some voters require the use of magnifiers to read the ballots on current voting machines. It may be inferred that some voters may therefore require the use of magnifiers to view the voter-verified paper record even if it adheres to the size standards. If these size standards are achieved by allowing built-in magnification on the machine then the use of additional magnification will be difficult for the voter.

Paper record fragility

Problem – The requirement of N.J.S.A. 19:53A-3.i that the paper record be "permanent" has been interpreted in VVPRC III.C.3 as "If stored in accordance with vendor specifications, the paper used to produce a paper record shall be readable for a period of at least two years after the election in which it is used.". This requirement has been implemented by the vendors and accepted by the VMEC by use of thermal printing paper for the paper record. I have been unable to find any vendor specifications on line and rely on testimony given at VMCE hearings such as that the paper is sensitive to excessive heat and light and that the specifications are "essentially are temperature and humidity that we find in this room and you can save some variation around that considering voting machines are stored in a warehouse environment which may not have perfect air conditions like at your house or in a business office.". These storage criteria seem reasonable but do not account for the possibility that either through negligence or intent to disrupt an election the paper records may be subject to extreme conditions of temperature, light, or chemical vapors rendering them unreadable.

Proposed Remedy – Conditions under which the paper records may be safely stored should be a specified requirement in the VVPRC. These specifications should include not only conditions under which the records are planned to be stored but also adverse conditions to which the records may be exposed such as excessive heat and exposure to chemical vapors commonly found in offices. The specifications supplied by the vendor should not relied upon but there should be independent testing to ensure that the paper meets the required specifications such as was done for the machines themselves.

Discussion – Thermal printing systems are highly reliable as they require few components and few

moving parts. However the output is notoriously fragile. The National Archives and Record Administration does not consider thermal paper to be permanent medium. The purpose of the requirement for a voter-verified paper record is to ensure that the ballots are secure against accidental or intentional tampering. The paper records themselves should therefore be secure against accidental or intentional tampering. They should be able to survive being left in a vehicle in the hot sun, being placed next to a steam radiator, being in a warehouse where someone with evil intent has turned off the air conditioning or turned up the thermostat, or being in a room where someone has left open a bottle of a cleaning chemical.

Sources and Additional Information

The VVPRC and VMEC hearing transcripts were obtained from http://www.nj.gov/state/elections/county-voting-equipment-vvpat.html

N.J.S.A. were obtained from http://lis.njleg.state.nj.us/nxt/gateway.dll?f=templates&fn=default.htm&vid=Publish:10.1048/Enu

The National Archives and Record Administration statement on thermal paper can be found at https://www.archives.gov/records-mgmt/bulletins/1996/96-03.html

White paper on thermal paper durability from Brother Mobile Solutions, Inc. https://www.brother-usa.com/Mobile/pdfs/white_papers/ThermalPaperWhitePaper.pdf

About Charles P. Lamb

• Resident of Scotch Plains, New Jersey.

• Served as a poll worker in Scotch Plains for approximately 25 years.

• Graduate of Case Western Reserve University with a B.S. in Computer Engineer.

• Graduate of New Jersey Institute of Technology with a M.S. in Computer Science.

• Professional developer of computer graphics systems.

ADDITIONAL APPENDIX MATERIALS
SUBMITTED TO THE

ASSEMBLY JUDICIARY COMMITTEE

for the
October 26, 2017 Meeting

Submitted by Reverend Robert Moore, Executive Director, Coalition for Peace Action**:**

Senator Linda R. Greensten and Rev. Robert Moore, "N.J. senator: Let's avoid a Russian hack, protect N.J.'s vote," *The Star-Ledger,* June 12, 2017. ©2017 New Jersey On-Line LLC.