

The State of Electronic Voting, 2008

David Wagner
UC Berkeley

ACCURATE



A CENTER FOR
CORRECT, USABLE,
RELIABLE, AUDITABLE,
AND TRANSPARENT ELECTIONS

David Wagner, UC Berkeley

An Abbreviated History of E-Voting



Confusion at Palm Beach County polls

Some Al Gore supporters may have mistakenly voted for Pat Buchanan because of the ballot's design.

Although the Democrats are listed second in the column on the left, they are the third hole on the ballot.

Punching the second hole casts a vote for the Reform party.

ELECTORS FOR PRESIDENT AND VICE PRESIDENT	
(REPUBLICAN) GEORGE W. BUSH - PRESIDENT DICK CHENEY - VICE PRESIDENT 3 →	(REFORM) PAT BUCHANAN - PRESIDENT EZOLA FOSTER - VICE PRESIDENT ← 4
(DEMOCRATIC) AL GORE - PRESIDENT JOE LIEBERMAN - VICE PRESIDENT 5 →	(SOCIALIST) DAVID McREYNOLDS - PRESIDENT MARY CAL HOLLIS - VICE PRESIDENT ← 6
(LIBERTARIAN) HARRY BROWNE - PRESIDENT ART OLIVIER - VICE PRESIDENT 7 →	(CONSTITUTION) HOWARD PHILLIPS - PRESIDENT J. CURTIS FRAZIER - VICE PRESIDENT ← 8
(GREEN) RALPH NADER - PRESIDENT WINONA LaDUKE - VICE PRESIDENT 9 →	(WORKERS WORLD) MONICA MOOREHEAD - PRESIDENT GLORIA La RIVA - VICE PRESIDENT ← 10
(SOCIALIST WORKERS) JAMES HARRIS - PRESIDENT MARGARET TROWE - VICE PRESIDENT 11 →	WRITE-IN CANDIDATE To vote for a write-in candidate, follow the directions on the long stub of your ballot card.
(NATURAL LAW) JOHN HAGELIN - PRESIDENT NAT GOLDHABER - VICE PRESIDENT 13 →	

(A vote for the candidates will actually be a vote for their electors.)
(Vote for Group)

From: Lana Hires

Subject: 2000 November Election

I need some answers! Our department is being audited by the County.

I have been waiting for someone to give me an explanation as to why Precinct 216 gave Al Gore a minus 16022 when it was uploaded. Will someone please explain this so that I have the information to give the auditor instead of standing here "looking dumb".

2000 Election Spurs Electoral Reform

Oct 2002: Congress passes Help America Vote Act (HAVA): states must upgrade voting systems by 2006; provides \$3.6 billion in federal funding.

HAVA accelerates adoption of e-voting.

DREs used by 13% of voters in 2000 → 38% in 2006

Sequoia Voting Systems



Hart InterCivic



Premier (was: Diebold)



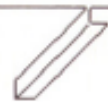


OFFICIAL GENERAL ELECTION BALLOT
SARASOTA COUNTY, FLORIDA
NOVEMBER 7, 2006

CONGRESSIONAL

UNITED STATES SENATOR
(Vote for One)

Katherine Harris	REP	<input type="checkbox"/>
Bill Nelson	DEM	<input type="checkbox"/>
Floyd Ray Frazier	NPA	<input type="checkbox"/>
Belinda Noah	NPA	<input type="checkbox"/>
Brian Moore	NPA	<input type="checkbox"/>
Roy Tanner	NPA	<input type="checkbox"/>
Write-In		<input type="checkbox"/>



U.S. REPRESENTATIVE IN CONGRESS
13TH CONGRESSIONAL DISTRICT
(Vote for One)

Vern Buchanan	REP	<input type="checkbox"/>
Christine Jennings	DEM	<input type="checkbox"/>

STATE

GOVERNOR AND LIEUTENANT GOVERNOR
(Vote for One)

Charlie Crist	REP	<input type="checkbox"/>
Jeff Kottkamp		
Jim Davis	DEM	<input type="checkbox"/>
Daryl L. Jones		
Max Linn	REF	<input type="checkbox"/>
Tom Macklin		
Richard Paul Dembinsky	NPA	<input type="checkbox"/>
Dr. Joe Smith		
John Wayne Smith	NPA	<input type="checkbox"/>
James J. Kearney		
Karl C.C. Behm	NPA	<input type="checkbox"/>
Carol Castagnero		
Write-In		<input type="checkbox"/>

ATTORNEY GENERAL
(Vote for One)

Bill McCollum	REP	<input type="checkbox"/>
Walter "Skip" Campbell	DEM	<input type="checkbox"/>

CHIEF FINANCIAL OFFICER
(Vote for One)

Tom Lee	REP	<input type="checkbox"/>
Alex Sink	DEM	<input type="checkbox"/>

COMMISSIONER OF AGRICULTURE
(Vote for One)

Charles H. Bronson	REP	<input type="checkbox"/>
Eric Copeland	DEM	<input type="checkbox"/>

Audience poll

Poll: How many contests did you vote in?


U.S. Congress Rep., Sarasota FL, Nov 2006

OFFICIAL GENERAL ELECTION BALLOT
SARASOTA COUNTY, FLORIDA
NOVEMBER 7, 2006

CONGRESSIONAL

UNITED STATES SENATOR
(Vote for One)

Katherine Harris	REP	<input type="checkbox"/>
Bill Nelson	DEM	<input type="checkbox"/>
Floyd Ray Frazier	NPA	<input type="checkbox"/>
Belinda Noah	NPA	<input type="checkbox"/>
Brian Moore	NPA	<input type="checkbox"/>
Roy Tanner	NPA	<input type="checkbox"/>
Write-In		<input type="checkbox"/>



Page 1 of 21
Public Count: 0

Next Page

U. S. REPRESENTATIVE IN CONGRESS
13TH CONGRESSIONAL DISTRICT
(Vote for One)

Vern Buchanan	REP	<input type="checkbox"/>
Christine Jennings	DEM	<input type="checkbox"/>

STATE

GOVERNOR AND LIEUTENANT GOVERNOR
(Vote for One)

Charlie Crist	REP	<input type="checkbox"/>
Jeff Kottkamp		
Jim Davis	DEM	<input type="checkbox"/>
Daryl L. Jones		
Max Linn	REP	<input type="checkbox"/>
Tom Macklin		
Richard Paul Dembinsky	NPA	<input type="checkbox"/>
Dr. Joe Smith		
John Wayne Smith	NPA	<input type="checkbox"/>
James J. Kearney		
Karl C.C. Behm	NPA	<input type="checkbox"/>
Carol Castagnero		
Write-In		<input type="checkbox"/>

Previous Page

Page 2 of 21
Public Count: 0

Next Page

Margin of victory: 369 votes (0.15% of voters)

No vote recorded: 18,412 votes (14% of e-voters)

U.S. Congress Rep., Sarasota FL, Nov 2006

Did voters see this?

OFFICIAL GENERAL ELECTION BALLOT
SARASOTA COUNTY, FLORIDA
NOVEMBER 7, 2006

CONGRESSIONAL

UNITED STATES SENATOR
(Vote for One)

Katherine Harris	REP	<input type="checkbox"/>
Bill Nelson	DEM	<input type="checkbox"/>
Floyd Ray Frazier	NPA	<input type="checkbox"/>
Belinda Noah	NPA	<input type="checkbox"/>
Brian Moore	NPA	<input type="checkbox"/>
Roy Tanner	NPA	<input type="checkbox"/>
Write-In		<input type="checkbox"/>

Page 1 of 21
Public Count: 0

Next Page

U. S. REPRESENTATIVE IN CONGRESS
13TH CONGRESSIONAL DISTRICT
(Vote for One)

Vern Buchanan	REP	<input type="checkbox"/>
Christine Jennings	DEM	<input type="checkbox"/>

STATE

GOVERNOR AND LIEUTENANT GOVERNOR
(Vote for One)

Charlie Crist	REP	<input type="checkbox"/>
Jeff Kottkamp		
Jim Davis	DEM	<input type="checkbox"/>
Daryl L. Jones		
Max Linn	REP	<input type="checkbox"/>
Tom Macklin		
Richard Paul Dembinsky	NPA	<input type="checkbox"/>
Dr. Joe Smith		
John Wayne Smith	NPA	<input type="checkbox"/>
James J. Kearney		
Karl C.C. Behm	NPA	<input type="checkbox"/>
Carol Castagnero		
Write-In		<input type="checkbox"/>

Previous Page

Page 2 of 21
Public Count: 0

Next Page

Margin of victory: 369 votes (0.15% of voters)

No vote recorded: 18,412 votes (14% of e-voters)

More than 4,500 North Carolina votes lost because of mistake in voting machine capacity

JACKSONVILLE, N.C. (AP) — More than 4,500 votes have been lost in one North Carolina county because officials believed a computer that stored ballots electronically could hold more data than it did. Scattered other problems may change results in races around the state.

Officials said UniLect Corp., the maker of the county's electronic voting system, told them that each storage unit could handle 10,500 votes, but the limit was actually 3,005 votes.

Machine error gives Bush 3,893 extra votes in Ohio

By John McCarthy, Associated Press

COLUMBUS, Ohio — An error with an electronic voting system gave President Bush 3,893 extra votes in suburban Columbus, elections officials said.

Franklin County's unofficial results had Bush receiving 4,258 votes to Democrat John Kerry's 260 votes in a precinct in Gahanna. Records show only 638 voters cast ballots in that precinct. Bush's total should have been recorded as 365.

Broward Vote-Counting Blunder Changes Amendment Result

POSTED: 1:34 pm EST November 4, 2004

BROWARD COUNTY, Fla. -- The Broward County Elections Department has egg on its face today after a computer glitch misreported a key amendment race, according to WPLG-TV in Miami.

Amendment 4, which would allow Miami-Dade and Broward counties to hold a future election to decide if slot machines should be allowed at racetracks, was thought to be tied. But now that a computer glitch for machines counting absentee ballots has been exposed, it turns out the amendment passed.

"The software is not geared to count more than 32,000 votes in a precinct. So what happens when it gets to 32,000 is the software starts counting backward," said Broward County Mayor Ilene Lieberman.

That means that Amendment 4 passed in Broward County by more than 240,000 votes rather than the 166,000-vote margin reported Wednesday night. That increase changes the overall statewide results in what had been a neck-and-neck race, one for which recounts had been going on today. But with news of Broward's error, it's clear amendment 4 passed.



Broward County Mayor Ilene Lieberman says voting counting error is an "embarrassing mistake."

We would like to explain in further technical detail what caused this issue, should you or others at the county have questions. The 32,767 capacity limitation at a single precinct level is a function of the design and definition of the results database used by ERM. The data storage element used to record votes at the precinct level is a two byte binary field. 32,767 is 2 to the 15th power, which is the maximum number held by a two byte word (16 bits) in memory, where the most significant bit is reserved as the sign bit (a plus or minus indicator). Additionally, ERM precinct count level data is stored in a binary computer format known as two's complement. Data on ERM results reports are printed as the absolute value of the two's complement of the associated data in the ERM database. This means that once the 32,767 limitation is reached, additional incremental tallies of vote results would not be printed correctly (32,768 through 65,536 would actually be represented as 65,536 to 32,768).

E-Voting Raises Security Concerns



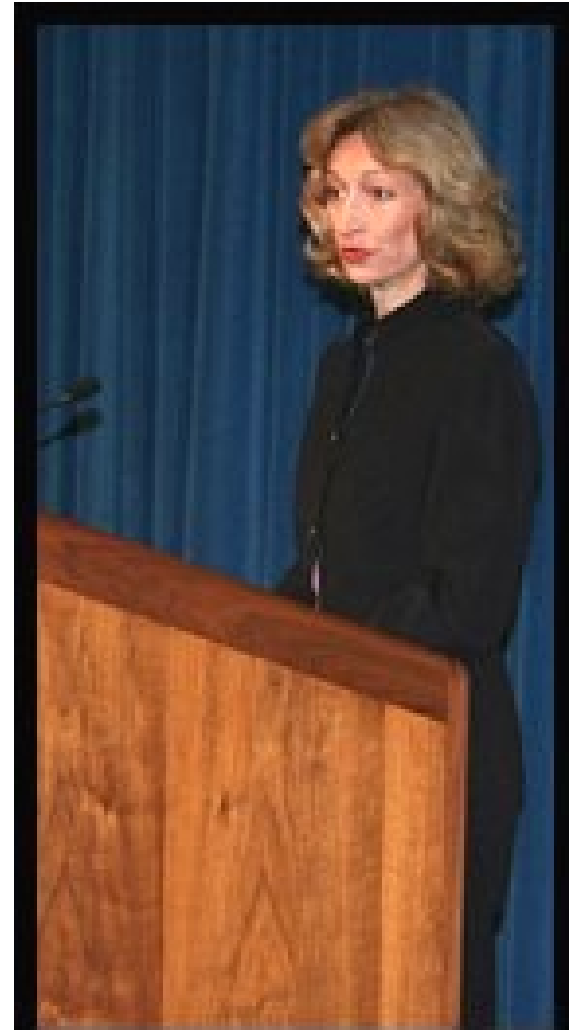


KEYS TO THE KINGDOM

Photo taken from Diebold's online store. The keys that open every Diebold touch-screen voting machine. Working copies have been made from the photo.

California Top-to-Bottom Review

Jun 2007: Secretary Bowen hires 43 experts to evaluate voting systems used in CA.



THE SECRETARY
Bowen opens the public hearing in Sacramento.

We found...

We found... significant security problems in all 3 systems.

Sequoia

Sequoia invented their own password encryption algorithm.

Sequoia

Sequoia invented their own password encryption algorithm. With the Sequoia algorithm, the password “**sekret**” encrypts to “**sekretXYZ**”*.

Sequoia

Sequoia invented their own password encryption algorithm. With the Sequoia algorithm, the password “**sekret**” encrypts to “**sekretXYZ**”^{*}.

^{*} Obfuscated for 'security'; “XYZ” are not the real letters.

Sequoia

“We could not find a single instance of correctly used cryptography that successfully accomplished the security purposes for which it was apparently intended.”

— Sequoia source team

Diebold

One of Diebold's passwords was

Diebold

One of Diebold's passwords was “**diebold**”.

Hart

In some places, Hart avoided trivially broken crypto by...

Hart

In some places, Hart avoided trivially broken crypto by...
omitting it entirely.

Hart

In some places, Hart avoided trivially broken crypto by... omitting it entirely.

When you connect a polling-place machine to the county's central PC, it trusts the PC implicitly.

The county PC can instruct the machine to overwrite its software, and it will blindly comply. (No authentication!)

The code fails to follow sound engineering principles expected of security-critical systems.

Diebold

```
void GlibPutPixel(UINT xx, UINT yy, Pixel_t color) {  
    // Check for library not initialized or (x,y) out of range  
    if(FrameBuffer != FALSE || (xx < USER_X) || (yy < USER_Y)) {  
        // Compute the frame buffer offset and write the pixel  
        FrameBuffer[FB_OFFSET(xx,yy)] = color;  
    }  
}
```

Diebold

```
TCHAR name;  
_stprintf(&name, _T("\\Storage Card\\%s"),  
    findData.cFileName);  
Install(&name, hInstance);
```

All 3 systems allow malicious code to propagate virally.

Diebold

The Diebold code that reads data off the memory card has buffer overruns and other vulnerabilities.

Diebold

1. Attacker writes malicious data onto a memory card.
2. Uploading results at county HQ on election night infects county machines.
3. Infected county machines write malicious data and code onto memory cards that will infect all polling-place machines in the county in the next election.

Hart

After the election, each polling-place machine is connected by Ethernet to a county PC. The PC can install new software onto the voting machine.

Hart

After the election, each polling-place machine is connected by Ethernet to a county PC. The PC can install new software onto the voting machine.

The voting machine can exploit buffer overruns in the code on the PC to take control of the PC.

Hart

1. Attacker installs malicious code onto a voting machine.
2. When connected to the county PC, it hacks the PC.
3. The county PC then installs malicious code onto every voting machine subsequently connected to it.

A single individual, with no special access, could introduce a virus onto a single voting machine,

A single individual, with no special access, could introduce a virus onto a single voting machine, and this virus could infect every machine in the county.

Results

In August 2007, California Secretary of State Debra Bowen decertified these systems.

Consequence: In 2008 elections, most California voters voted on paper ballots.

So, How Did We Do In 2008?

2008 Elections

We were fortunate; there seem to have been no major fiascos in the 2008 election.

Problem areas: equipment failures, long lines, registration matching issues.

Results tape from Bergen County, NJ, Feb. 2008

$$33 + 49 + 2 = 84 \text{ Democratic votes}$$

Candidate	Candidate Totals	Total
***	REPUBLICAN	***
*	US President C11	(1)
D11	Rudw Giuliani	1
E11	Ron Paul	1
F11	Fred Thompson	0
G11	Mitt Romney	6
H11	Mike Huckabee	0
I11	John McCain	14
B11	Personal Choice	0

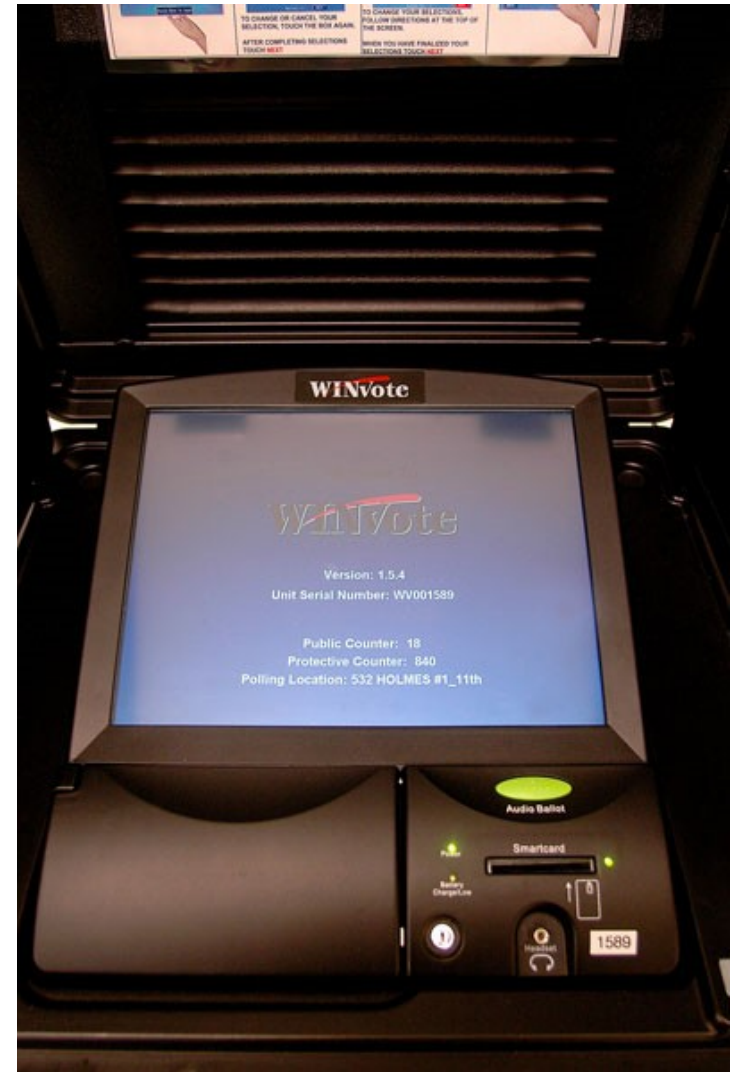
***	DEMOCRAT	***
*	US President- 19th Dist C18	(1)
D18	Barack Obama	33
E18	Joe Biden	0
F18	John Edwards	2
G18	Hillary Clinton	49
H18	Dennis Kucinich	0
I18	Bill Richardson	0
J19	Uncommitted	0
B18	Personal Choice	0

Write In Votes
No Write In Votes In Memory

Option Switch Totals

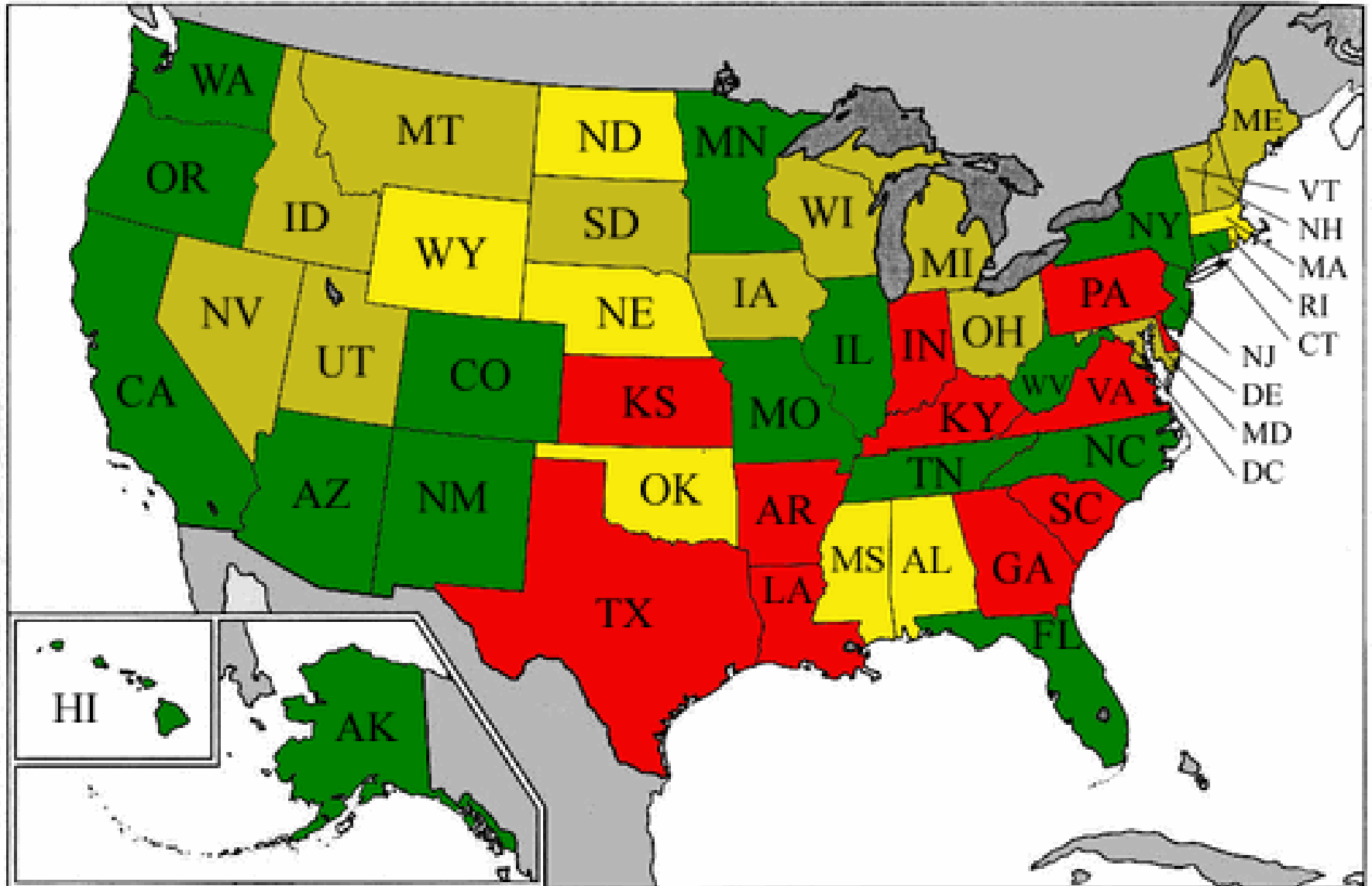
1	UNUSED	0
2	UNUSED	0
3	UNUSED	0
4	UNUSED	0
5	UNUSED	0
6	REPUBLICAN	0
7	UNUSED	0
8	UNUSED	0
9	UNUSED	0
10	UNUSED	0
11	UNUSED	0
12	DEMOCRAT	22
Total		83
		105

83 Democratic voters



How Do Things Stand Going Forward?

Auditability and Recountability



Concluding thoughts

- Elections are a complex distributed system, with equipment operated and administered by volunteers
- Despite its imperfections, electronic voting can be trusted if it can be audited