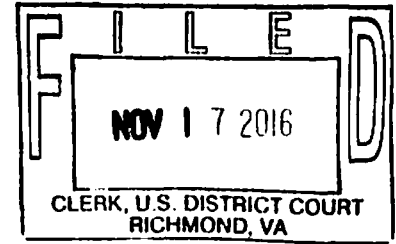


**IN THE UNITED STATES DISTRICT COURT
FOR THE
EASTERN DISTRICT OF VIRGINIA**



"STATES" MANSHIP, James Renwick Manship
Box 1776, Mount Vernon, Virginia 22121-1776
Plaintiff,

v.

No. 3:16-cv-00884

VIRGINIA BOARD OF ELECTIONS

JAMES B. ALCORN, in his official capacity as
Chairman of the Virginia State Board of Elections,
CLARA BELLE WHEELER, in her official capacity as
Vice Chairman of the Virginia State Board of Elections,
SINGLETON McALLISTER, in her official capacity as
Secretary of the Virginia State Board of Elections, and
EDGARDO CORTES, in his official capacity as
Commissioner of the Virginia Department of Elections, and
TERRENCE McAULIFFE, in his official capacity as
Governor of the Commonwealth of Virginia,
Defendants.

**MOTION TO RECONSIDER DISMISS WITH PREJUDICE ORDER FOR INJUNCTIVE
AND DECLARATORY RELIEF and VERIFIED CLASS ACTION COMPLAINT**

1. Plaintiff respectfully moves the Court to reconsider its Order to Dismiss with Prejudice the Plaintiff's Emergency Motion filed on 1 November, a week in advance of the 2016 Election, that constituted the emergency request. The 2016 Election is complete, yet the underlying risks raised by the Plaintiff's complaint remain. In support of that reality of risks is given the Harvard Kennedy School of Government lecturer and chief technology officer of the cyber-security company Resilient, and the author of "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World", Bruce Schneier, Op-Ed in The New York Times the day after:

American Elections Will Be Hacked By BRUCE SCHNEIER NOV. 9, 2016

CAMBRIDGE, Mass. — It's over. The voting went smoothly. As of the time of writing, there are no serious fraud allegations, nor credible evidence that anyone hacked the voting rolls or voting machines. And most important, the results are not in doubt.

While we may breathe a collective sigh of relief about that, we can't ignore the issue until the next election. The risks remain.

As computer security experts have been saying for years, our newly computerized voting systems are vulnerable to attack by both individual hackers and government-sponsored cyberwarriors. It is only a matter of time before such an attack happens.

Electronic voting machines can be hacked, and those machines that do not include a paper ballot that can verify each voter's choice can be hacked undetectably. Voting rolls are also vulnerable; they are all computerized databases whose entries can be deleted or changed to sow chaos on Election Day.

The largely ad hoc system in states for collecting and tabulating individual voting results is vulnerable as well. While the difference between theoretical if demonstrable vulnerabilities and an actual attack on Election Day is considerable, we got lucky this year. Not just presidential elections are at risk, but state and local elections, too.

To be very clear, this is not about voter fraud. The risks of ineligible people voting, or people voting twice, have been repeatedly shown to be virtually nonexistent, and "solutions" to this problem are largely voter-suppression measures. Election fraud, however, is both far more feasible and much more worrisome.

Here's my worry. On the day after an election, someone claims that a result was hacked. Maybe one of the candidates points to a wide discrepancy between the most recent polls and the actual results. Maybe an anonymous person announces that he hacked a particular brand of voting machine, describing in detail how.

Or maybe it's a system failure during Election Day: voting machines recording significantly fewer votes than there were voters, or zero votes for one candidate or another. (These are not theoretical occurrences; they have both happened in the United States before, though because of error, not malice.)

We have no procedures for how to proceed if any of these things happen. There's no manual, no national panel of experts, no regulatory body to steer us through this crisis. How do we figure out if someone hacked the vote? Can we recover the true votes, or are they lost? What do we do then?

First, we need to do more to secure our elections system. We should declare our voting systems to be critical national infrastructure. This is largely symbolic, but it demonstrates a commitment to secure elections and makes funding and other resources available to states.

We need national security standards for voting machines, and funding for states to procure machines that comply with those standards. Voting-security experts can deal with the technical details, but such machines must include a paper ballot that provides a record verifiable by voters.

The simplest and most reliable way to do that is already practiced in 37 states: optical-scan paper ballots, marked by the voters, counted by computer but recountable by hand. And we need a system of pre-election and postelection security audits to increase confidence in the system.

Second, election tampering, either by a foreign power or by a domestic actor, is inevitable, so we need detailed procedures to follow — both technical procedures to figure out what happened, and legal procedures to figure out what to do — that will efficiently get us to a fair and equitable election resolution.

There should be a board of independent computer-security experts to unravel what happened, and a board of independent election officials, either at the Federal Election Commission or elsewhere, empowered to determine and put in place an appropriate response.

In the absence of such impartial measures, people rush to defend their candidate and their party. Florida in 2000 was a perfect example. What could have been a purely technical issue of determining the intent of every voter became a battle for who would win the presidency.

The debates about hanging chads and spoiled ballots and how broad the recount should be were contested by people angling for a particular outcome. In the same way, after a hacked election, partisan politics will place tremendous pressure on officials to make decisions that override fairness and accuracy.

That is why we need to agree on policies to deal with future election fraud. We need procedures to evaluate claims of voting-machine hacking. We need a fair and robust vote-auditing process. And we need all of this in place before an election is hacked and battle lines are drawn.

In response to Florida, the Help America Vote Act of 2002 required each state to publish its own guidelines on what constitutes a vote. Some states — Indiana, in particular — set up a “war room” of public and private cybersecurity experts ready to help if anything did occur. While the Department of Homeland Security is assisting some states with election security, and the F.B.I. and the Justice Department made some preparations this year, the approach is too piecemeal.

Elections serve two purposes. First, and most obvious, they are how we choose a winner. But second, and equally important, they convince the loser — and all the supporters — that he or she lost.

To achieve the first purpose, the voting system must be fair and accurate.

To achieve the second one, it must be *shown* to be fair and accurate.

We need to have these conversations before something happens, when everyone can be calm and rational about the issues. The integrity of our elections is at stake, which means our democracy is at stake.

2. Virginia has made progress since the election of 2012, when this Plaintiff filed a Complaint after election day, but prior to the counting of the Elector Votes, that was NOT Dismissed with Prejudice, by the same Judge. Virginia did largely replace the DRE “Touch Screen” voting machines (What per cent? Where are the DRE machines still in use? Why?) that were woefully vulnerable to electronic hacking, replaced with the printed paper ballot that is scanned by an electronic device for counting — with **the saving grace** of the post-2012 scanned paper ballot system being that should someone question the electronic machine vote count — then **the printed paper ballots can be hand-counted**.
3. Yet as to the Voter’s two part Right to Vote under *Reynolds v. Sims*, of (1) Right to cast a ballot, and (2) Right to know that the vote and others were honestly counted, who under Virginia Code is “authorized” or “empowered” to question the vote count? A Party? Candidate? Or a mere Voter? Or many mere Voters? The WikiLeaks emails of the Democrat Party show the Party had a preferred Candidate, and the calls and cries of Electronic Vote Fraud by losing Candidate Sanders and his many supporters were ignored. So this is not a Republican versus Democrat issue, it is an overall Election Integrity issue.

4. In the Plaintiff's Mount Vernon Precinct of Belle View on Election Day 2016, more than one ES&S Electronic Scanner Voting Machine was used, and the plaintiff asked permission to take a photo of one machine, that request was granted. During that photo taking, Plaintiff also noticed that the back panel was open to "the air".
5. Cyber-Security experts have testified that such open air access can be used by a technically skilled agent in a matter of seconds to insert a code card such that the Electronic Voting Machine that scans printed ballots can be re-programmed to perform "Decimalization of Votes"¹ per Voting expert, Democrat Bev Harris who mentions in her summary both **Virginia** and the **Election Systems & Software (ES&S)** equipment:

1 – SUMMARY –

This report summarizes the results of our review of the **GEMS election management system, which counts approximately 25 percent of all votes in the United States**. The results of this study demonstrate that a **fractional vote feature is embedded in each GEMS application which can be used to invisibly, yet radically, alter election outcomes by pre-setting desired vote percentages to redistribute votes**. This tampering is not visible to election observers, even if they are standing in the room and watching the computer. Use of the decimalized vote feature is **unlikely to be detected by auditing or canvass procedures, and can be applied across large jurisdictions in less than 60 seconds**.

GEMS vote-counting systems are and have been operated under five trade names: Global Election Systems, Diebold Election Systems, Premier Election Systems, Dominion Voting Systems, and **Election Systems & Software**, in addition to a number of private regional subcontractors. At the time of this writing, **this system is used statewide in Alaska, Connecticut, Georgia, Mississippi, New Hampshire, Utah and Vermont, and for counties in Arizona, California, Colorado, Florida, Illinois, Indiana, Iowa, Kansas, Kentucky, Massachusetts, Michigan, Missouri, Ohio, Pennsylvania, Tennessee, Texas, Virginia**, (Plaintiff's Note: Which counties in Virginia?), Washington, Wisconsin and Wyoming. It is also used in Canada.

¹<http://blackboxvoting.org/fraction-magic-1/>

Fractionalized vote:

Instead of “1” the vote is allowed to be $1/2$, or $1+7/8$, or any other value that is not a whole number.

What fractionalized votes can do:

They allow “weighting” of races. **Weighting a race removes the principle of “one person-one vote”** to allow some votes to be counted as less than one or more than one. Regardless of what the real votes are, candidates can receive a set percentage of votes. Results can be controlled. For example, Candidate A can be assigned 44% of the votes, Candidate B 51%, and Candidate C the rest.

GEMS fractionalizes votes in three places:

The “**Summary**” vote tally, which provides overall election totals for each race on Election Night

The “**Statement of Votes Cast**”, which provides detailed results by precinct and voting method (ie. Polling, absentee, early, provisional)

The “**undervote**” count

Fractions in results reports are not visible. Votes containing decimals are reported as whole numbers unless specifically instructed to reveal decimals (which is not the default setting).

All evidence that fractional values ever existed can be removed instantly even from the underlying database using a setting in the GEMS data tables, in which case even instructing GEMS to show the decimals will fail to reveal they were used.

Source code: Instructions to treat votes as decimal values instead of whole numbers are inserted multiple times in the GEMS source code itself; thus, this feature cannot have been created by accident.

Fractionalizing the votes which create the Summary Results allows alteration of Election Night Web results and results sent to the Secretary of State, as well as results available at and local election officials.

Fractionalizing the “Statement of Votes Cast” allows an extraordinary amount of precision, **enabling alteration of results by specific voting machine, absentee batch, or precinct.** Vote results can be altered for polling places in predominantly Black neighborhoods, and can parse out precincts within a mixed batch of early or absentee votes.

Fractionalizing the undervote category allows reallocation of valid votes into undervotes.

6. Voting expert Democrat Bev Harris goes on to inform concerned Americans about race weighted features of GEMS election software that are distressing to learn:

Voting rights abomination

According to programmer notes, a weighted race feature was designed which not only gives some votes more weight than others, but does so based on the voter's identity. Ballots are connected to voters, weights are assigned to each voter per race, stored in an external table not visible in GEMS. **Our testing shows that one vote can be counted 25 times, another only one one-thousandth of a time, effectively converting some votes to zero.**

The study was prompted by two issues:

- (1) Anomalies in elections in Shelby County, Tennessee, which uses the GEMS election management system, in which inconsistencies were observed in reporting of results by GEMS; and
- (2) Concerns raised regarding the presence of middlemen during the election process, such that a single individual gains remote access to the election management program, in some cases in multiple jurisdictions.

The questions we examine are these:

Can election outcomes be controlled with enough versatility to allow a national impact?

Does any mechanism exist that would enable a political consultant or technician to capture elections for repeat customers?

If the necessary features exist within the election management system to facilitate this:

Were such features embedded accidentally or on purpose; for what stated purpose were such features installed; if a reason was given, is that reason justifiable?

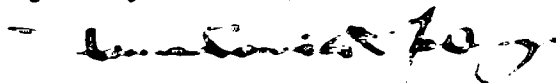
How might risks associated with inside access be mitigated?

The Court's ORDER of INJUNCTION against the Defendant Virginia Board of Elections should require per Virginia Code a Multi-Jurisdictional Grand Jury of randomly selected private citizens, with private counsel, empowered to employ cyber-security experts to answer the above questions, and questions the Grand Juror Citizens pose from their investigations.

7. Further, the ORDER OF INJUNCTION should direct that the results of the (Special) Multi-Jurisdictional Grand Jury be provided to every member of the General Assembly, Senate and House of Delegates, so that necessary changes in the Virginia Code can be undertaken in a careful, responsible, cyber-security informed, deliberative process thereafter to be in place prior to the next General Election in November 2017, for while the Grand Jury investigative report may have been completed, it is unlikely the General Assembly can rewrite laws in time, then pass the new laws with a majority of both houses, with those new laws signed, not vetoed, by the Defendant Governor, in time for Virginia's Primary Elections in June 2017.

8. It may be wise for the Court in its ORDER OF INJUNCTION, to specify that eleven, rather than the minimum of seven, in accordance with "Virginia Code § 19.2-215.4. Number and qualifications of jurors; grand jury list; when convened; compensation of jurors.", randomly selected private citizens be chosen from multiple jurisdictions for the Multi-Jurisdictional Grand Jury to be fairly distributed between county and city jurisdictions, some from large population counties (Chesterfield or Fairfax), or cities (Virginia Beach or Alexandria), and small population counties and cities, be regionally geographically diverse, urban and rural, and even consider a balance of members based on the jurisdiction's past voting patterns of Democrat dominant voting or Republican dominant voting, so there is increased chance of the Multi-Jurisdictional Grand Jury's investigation to be free from party preference or regional bias.

Respectfully submitted,



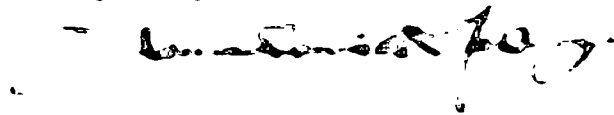
James Renwick Manship, Plaintiff, *Pro Se*
LCDR, USNR, Special Duty, Cryptology
Box 1776, Mount Vernon, Virginia 22121-1776
703-672-1776
StatesManship@me.com

CERTIFICATE OF SERVICE

In accordance with the provisions of U.S. Marshall conducted Service for *In Forma Pauperis* litigants, Plaintiff Manship, who as a Disabled Navy Veteran whose disability pension has been interrupted in past years at times exists on the grace of God through a few Children of God, and has previously qualified for *In Forma Pauperis* status with the federal district courts, and has been in this case approved by this same judge to proceed *In Forma Pauperis*, here requests that such be done for this case, and states that a Courtesy Copy will be mailed by First Class United States Postal Service on this day or the next depending on times of operation of copy centers to make duplicates and times of the Post Office for posting the documents.

DATED: 15 November *anno domini* 2016

Respectfully submitted,

A handwritten signature in black ink, appearing to read "James Renwick Manship", with a stylized flourish at the end.

James Renwick Manship, Plaintiff, *Pro Se*
LCDR, USNR, Special Duty, Cryptology
Box 1776, Mount Vernon, Virginia 22121-1776
703-672-1776
StatesManship@me.com

MAJOR STATESMANSHIP

BOX 1776

MOUNT VERNON, VA 22121-1776



FERNANDO GALINDO
CLERK OF COURT
U.S. DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
701 EAST BROAD STREET
RICHMOND, VA 23219

U.S. MARSHAL SERVICE
INSPECTOR