

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRIAN KEMP, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

**COALITION PLAINTIFFS' REPLY BRIEF IN SUPPORT OF
MOTION FOR PRELIMINARY INJUNCTION**

August 20, 2018

Table of Contents

I.	INTRODUCTION AND SUMMARY	1
II.	ARGUMENT	4
A.	Coalition Plaintiffs Are Likely to Succeed on the Merits	4
1.	DRE voting machines are profoundly insecure and vulnerable.....	5
2.	Georgia’s DRE Machines are Particularly Vulnerable.....	6
3.	Evidence of Malfunctions in Recent Elections	10
4.	Conclusion: Clear Likelihood of Success on the Merits	12
B.	Injunction Is in the Public Interest	12
1.	Proposed Remedy – Paper Ballots	13
2.	Proposed Remedy – Verification of Accuracy of Electronic Pollbooks	20
3.	Significant cost savings and federal funding	21
C.	Defendants’ Other Arguments are Without Merit	21
1.	Absentee Voting is Not a Constitutionally Adequate Alternative Remedy.....	21
2.	Effective relief may be granted against these Defendants.....	24
3.	The laches defense does not apply	27
4.	Old cases about DRE machines are not relevant.....	29
5.	Mandatory preliminary injunctive relief is appropriate.....	29
III.	Conclusion	30
	CERTIFICATE OF SERVICE	33

Plaintiffs Coalition for Good Governance, William Digges III, Laura Digges, Megan Missett, and Ricardo Davis (the “Coalition Plaintiffs”) file this Reply Brief in Support of their Motion for Preliminary Injunction. (Doc. 258).

I. INTRODUCTION AND SUMMARY

Defendants make no effort to defend the security or reliability of DRE machines or to rebut the unanimous and urgent recommendation of computer scientists and national security authorities that paperless DRE machines never be used in American elections again. Defendants also do not dispute that, with more time and more money, paper ballots are *the* solution to providing a secure, reliable, and verifiable voting system for Georgians. Instead, Defendants contend that — having ignored urgent warnings for years — they now have neither the will, time nor the money to protect their citizens’ constitutional rights. This response is insufficient as a matter of law: if a State causes the constitutional violation, it cannot escape the imposition of an effective remedy simply by saying that doing the right thing is too hard, whether it is segregated schools,¹ overcrowded prisons,² or unconstitutionally deficient voting systems.³

¹ *Swan v. Charlotte-Mecklenburg Bd. of Educ.*, 402 U.S. 1, 15 (1971) (“Once a right and a violation have been shown, the scope of a district court’s equitable powers to remedy past wrongs is broad, for breadth and flexibility are inherent in equitable remedies.”)

² *Brown v. Plata*, 563 U.S. 493 (2011) (affirming reduction of prison population as remedy for unconstitutional prison conditions).

³ *NAACP v. Cortes*, 591 F. Supp. 2d 757, 763, 768 (E.D. Pa. 2008) (granting injunctive relief, rejecting as factually unfounded defendants’ arguments that changing election rules would “cause chaos and confusion”).

Moreover, Defendants' protestations and declarations concerning the difficulty of using paper ballots fundamentally mischaracterizes the reasonable, prudent, and minimalist relief of polling place paper ballots the Coalition Plaintiffs seek in this Motion. Without doubt, changing Georgia's entire election process would be as challenging as it is unnecessary. The Coalition Plaintiffs are not seeking anything close to a major change in the election process, but instead a very specific change in *one step* of the process that will most likely *save* the State time and money — using paper ballots in the polling places instead of DREs to record voters' choices. The only change that a voter will notice as a result of this change is that, rather than touching an electronic screen, the voter will use a felt-tip pen to record his or her vote on a paper ballot and will place the paper ballot in a secure ballot box. To suggest that this minor change to the voting experience will cause mass chaos and voter confusion is utterly ridiculous.

Granting the requested relief means the Defendants will have to increase the quantity of paper ballots being printed, but the largest ballot printer in the country is ready, willing and able to provide as many ballots as Georgia needs for twenty-six cents a ballot.⁴ (Martin Decl., attached hereto as Exhibit D, ¶ 39). Evidence establishes that little if any additional training of poll worker staff is necessary; poll workers are already trained to securely handle and account for paper ballots

⁴ Richmond County is currently paying \$.35 per ballot. (Doc. 265-6 ¶ 8).

for provisional voters. (See R. Wilson Decl. ¶¶ 13-17, at Doc. 258-1, page 298-299). The labor intensive efforts of setting up, testing, securing, closing down, and transporting numerous DRE machines in every polling place are not necessary. (*Id.*). If additional scanners are desired to be added to the approximately 900 that are already in use in Georgia now (Doc. 265, page 8), used Accu-Vote scanners are widely available and can be purchased easily for reasonable amounts. (McReynolds Decl., attached hereto as Exhibit E, ¶ 48; Martin Decl., attached hereto as Exhibit D ¶ 44). Although Defendants complain that new equipment that may be needed has not been budgeted, they do not disclose the recent \$10.3 million in federal election security funding that was just granted to Georgia. The additional cost of the paper ballots and additional scanning machines, if needed, will be more than offset by the enormous savings associated with not having to test, program, transport, set up, take down and secure 27,000 DRE machines, and to handle and account for tens of thousands of DRE memory cards. Any administrative inconvenience Defendants may face in accommodating the Coalition Plaintiffs' requested remedy pales in comparison to the imminent harms and irreparable injury to voters that will be avoided. *See Brown*, 563 U.S. at 531 (“a narrow and otherwise proper remedy for a constitutional violation is not invalid simply because it will have collateral effects”).

II. ARGUMENT

The Coalition Plaintiffs will first address in Part A the overwhelming evidence establishing the likelihood of success on the merits and then, mindful of the Court’s focus on the practicality of injunctive relief, will address in Part B the proposed remedy in detail. In Part C, the Coalition Plaintiffs will address other arguments advanced by the Defendants, including the alleged availability of alternative relief, laches, the availability of mandatory preliminary injunctive relief, and other issues.

A. Coalition Plaintiffs Are Likely to Succeed on the Merits

Secretary Kemp’s failure to muster any rebuttal to Plaintiffs’ evidence leaves an evidentiary record that compels a finding that Plaintiffs are likely to succeed on the merits. Rather than attempt to defend the security of Georgia’s election system with evidence and reasoned analysis, Secretary Kemp instead insults the citizens who bring this claim and mocks the professionals who provide scientific evidentiary support.⁵ This all-too familiar tactic—insult the critic, ignore the facts and science—has no place in a court of law and by now serves only to

⁵ The State Defendants state that Plaintiffs harbor “[I]udite prejudices,” an ironic description given the Defendants’ refusal to address the overwhelming computer science authorities on the subject. The State Defendants, having no voting systems experts of their own, call Plaintiffs’ Expert Matthew Barnhart a “so-called expert” and a mere “Ph.D. candidate” (at Michigan); refer to Logan Lamb, who exposed the insecurity of the KSU server and immediately reported it to KSU, as a “hacker;” and call Rebecca Wilson, the Republican Chief Election Judge in Prince George County, Maryland, as a “lower-level functionar[y].” (Doc. 265 at pages 11-12).

emphasize the Secretary's inability to dispute the genuine threat that hangs over Georgia's upcoming mid-term elections.

What follows is a summary of Plaintiffs' evidence and Defendants' meager, if not nonexistent, rebuttal.

1. DRE voting machines are profoundly insecure and vulnerable.

In their opening Brief, Plaintiffs showed that the entire computer science community has concluded that DRE voting machines are unreliable, unquestionably insecure, and unverifiable. (Coalition Plaintiffs' Brief at 10 (Doc. 258-1, p. 12). The State Defendants denigrate Plaintiffs' experts, but do not submit any expert testimony of their own and do not address, much less refute, Plaintiffs' expert testimony or the mountains of academic and scholarly literature supporting their conclusions.

In their Brief, Plaintiffs explained that federal officials at the highest levels have unanimously urged that DRE machines be replaced with systems that have voter-verifiable paper trails.⁶ House Intelligence Committee Chairman Devin Nunes called for a complete ban on electronic voting;⁷ Director of Homeland Security Kirstjen Nielsen stated that using DRE machines presents a "national

⁶ As Director of Homeland Security Kirstjen Nielsen recently testified: "You must have a way to audit and verify the election result." (Doc. 258-1, n. 3).

⁷ <http://thehill.com/hilltv/rising/398949-house-intel-chair-calls-for-ban-on-electronic-voting-systems>.

security concern.”⁸ Select committees from the House⁹ and Senate¹⁰ issued detailed reports outlining the dangers of using paperless DREs and urgently recommending that DRE voting machines be abandoned.

Defendants do not address or dispute the conclusions reached by these federal officials, nor do they identify any government official (state or federal), voting system computer scientist, or cybersecurity expert who is willing to say to this Court on the record that DRE voting machines can be safely and reliably used to conduct public elections in Georgia.¹¹

2. *Georgia’s DRE Machines are Particularly Vulnerable.*

In their Brief, Plaintiffs explained that the already unacceptable extreme vulnerability of Georgia’s system was greatly increased by Secretary Kemp’s failure to secure the State’s central election server before and after the 2016 elections. This neglect that rendered Georgia’s entire voter registration database, the personal records of every Georgia voter, and the State’s election software and passcodes “fully accessible to any computer user with Internet access.” (Doc. 258-

⁸Doc. 258-1, n. 3.

⁹Doc. 258-1, n. 7.

¹⁰ Doc. 258-1, n. 5.

¹¹ Even the Secretary’s Chief Information Officer, Merritt Beaver, does not dispute the insecurity of the DRE voting machines, testifying instead that replacing DRE voting machines will not make the other components of the system more secure. (Doc. 265-1, page 5, ¶ 7). Yet, as expert Matthew Bernhard states: “The chain of security is only as strong as its weakest link, and the chain of election security in Georgia is all but broken due entirely to the insecurity of Georgia’s DRE voting machines.” (M. Bernhard Second Decl., filed herewith, ¶ 7).

1, page 15). Defendants do not disagree with this account, nor do they point to any evidence of attempted remediation of the extreme risk to which the entire system has been—and continues to be—exposed. As Matthew Barnhard explains in his Second Declaration: once a system is hacked, malware “thereafter can remain silently hidden.” (M. Bernhard Second Decl., attached hereto as Exhibit A, ¶ 10).

Plaintiffs also explained that, even after the Secretary’s agents were notified that the central election server was exposed to the public, “for reasons that have never been explained,” “between at least August 2016 and March 2017” the server and all of its election data and programming was left exposed to unauthorized access by anyone, anywhere in the world, with an internet connection. Secretary Kemp’s own agents at KSU warned that the compromised server was exploitable because of its “critical and severe vulnerabilities.” (Doc. 258-1, page 236). In their response brief, Defendants provide no explanation for this egregious neglect, nor do they express any intention to undertake essential forensic investigations remediate the risks introduced by their security failures.

Rather than responsibly addressing the security of Georgia’s systems, Defendants ridicule the Coalition Plaintiffs for raising the likelihood of “undetectable manipulation.” Betraying a total lack of knowledge or even interest in the threats to Georgia’s election system, and stunning arrogance, Defendants

state: “Evidence of ‘undetectable manipulation’ is oxymoric.” (Doc. 265, page 11). To the contrary: undetectable manipulation, a term of art in the computer science field, is today exactly what concerns experts the most about Georgia’s DRE voting system. This is explained in the Declaration of Dr. Richard DeMillo, the Charlotte B. and Roger C. Warren Professor of Computing and Professor of Management at Georgia Tech, attached hereto as Exhibit C. Dr. DeMillo states: “Undetectable manipulation is the most common, widely recognized, and serious threat facing computer systems, including election systems. . . . [T]he threat is not speculative or theoretical but rather is the fundamental building block of modern cyber security and cyber warfighting.” (DeMillo Decl. ¶ 11). Dr. DeMillo goes on to explain in authoritative detail undetectable manipulation and the threat it poses to Georgia’s election system. Dr. DeMillo concludes:

As these citations make clear, undetectable manipulation is a grave threat to Georgia’s paperless DRE voting system because APTs have plainly targeted the American election system, including in all likelihood Georgia’s system. It is well within the capabilities and consistent with usual practice of those APTs to utilize undetectable manipulation. Given the inability of the State to determine with any certainty whether the software presently being utilized by Georgia’s DRE voting system has been maliciously altered at any point in the past, it will be impossible for Georgians to have any reasonable degree of confidence in the integrity of the election results produced by Georgia’s DRE voting system.

(DeMillo Decl. ¶ 20uy). Because of the real threat of undetectable manipulation, “[t]he only known robust mechanism for universally disclaiming election malfunction is a physical paper record.” (Second M. Bernhard Decl., ¶ 7).

Defendants, quoting the Secretary’s Chief Information Officer Merritt Beaver, state that “[t]he way that KSU stored and transmitted data is not the way that those tasks are undertaken now,” (Doc. 265, page 30). This bland observation gives no assurance that the system is any more secure now than it was in the immediate aftermath of its months-long exposure to the world by KSU. Worse, saying that things have changed this misses the point entirely, for the issue is not (or not only) whether the system can be infiltrated anew, but is instead whether anything has ever been done to mitigate the catastrophic security failure that it known to have been suffered.

There is no evidence in the record that the Secretary has conducted or indeed *ever* intends to conduct a forensic examination to determine whether Georgia’s election system was altered or manipulated in the (at least) six months it was left exposed, six months that happens to overlap with the time period in which Russian operatives are alleged to have been probing for vulnerabilities in, and trying to manipulate, America’s election systems.¹² (Doc. 258-1 at 13). The Secretary’s failure to secure the server in the first place was negligent, but conducting an

¹² *United States v. Netyksho, et al.*, Indictment (D.D.C., July 13, 2018) ¶ 75

election using the same software that was stored on that server after that exposure, without first determining whether the server has been maliciously infiltrated, is reckless in the extreme.¹³

3. *Evidence of Malfunctions in Recent Elections*

Defendants do not even acknowledge, much less attempt to address, any of the alarming new evidence that Georgia's DRE voting system has inexplicably malfunctioned in recent 2016 through 2018 elections, particularly with respect to discrepancies between the Diebold electronic pollbooks (part of the certified DRE system) and the Secretary of State's official voter registration records. (Doc. 258-1, Clark Decl. ¶¶ 10-15 and Bowers Decl. ¶¶ 35-46). This silence amounts to a concession that the Secretary has no earthly idea why his election system is not working the way it is supposed to for so many Georgia voters. Whistling past the graveyard is not a suitable response in the face of real evidence of ongoing malfunctions, discrepancies, and irregularities affecting real Georgia voters who are attempting to exercise their fundamental right to vote.

¹³ In their Brief, Plaintiffs further explained that the vulnerability of DREs can be exploited whether or not the machines are directly connected to the internet in a live connection. (Doc. 258-1, p. 13). Secretary Kemp has claimed in the press: "State voting systems are diverse, highly scrutinized and not connected to the Internet. Web-based attacks on voter registration do not affect the vote count. The thing that matters most — your vote — is secure." B. Kemp, "States Keep Our Election Secure," USA Today, July 2, 2017. Plaintiffs are unaware of any factual support for Secretary Kemp's statement.

Indeed, not only is the Secretary mute in the face of the compelling evidence that the Coalition Plaintiffs have proffered, but the Secretary's conduct in this litigation supports an inference that whatever evidence the Secretary might have once possessed is detrimental to his defense. The Secretary's agents destroyed evidence by wiping the primary *and* secondary KSU servers *after* this litigation was filed, in plain violation of duties to preserve potentially relevant evidence. The Secretary assails any suggestion that his office might have spoliated evidence as "spurious," "mudslinging," and a "gimmick to distract." But the facts, which none of the Defendants contests, establish spoliation by the Secretary as a matter of law. *Kraft Reinsurance Ireland, Ltd. v. Pallets Acquisitions, LLC*, 845 F. Supp. 2d 1342, 1358 (N.D. Ga. 2011) ("Spoliation is the destruction...of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation."). Defendants inexplicably excuse themselves from having to present evidence by asserting that "certain parts of Georgia's elections infrastructure must remain secret" pursuant to an unidentified "state secrets doctrine." This outlandish claim, made without any citation to legal authority, is the crowning testament to the Secretary's complete inability to defend the security of DREs with anything other than invective and evidence-free, ad hominem argument.

4. *Conclusion: Clear Likelihood of Success on the Merits*

The substantially un rebutted evidence presented by Plaintiffs unquestionably warrants a finding that Plaintiffs are likely to succeed on the merits of their claim *and* that using the DRE machines in the upcoming election is not a responsible or constitutional option. “Once a constitutional violation is found, a federal court is required to tailor ‘the scope of the remedy’ to fit ‘the nature and extent of the constitutional violation.’” *Hills v. Gautreaux*, 425 U.S. 284, 293–94 (1976).

B. Injunction Is in the Public Interest

Before addressing the feasibility of the Coalition Plaintiffs’ proposed remedy, it is crucial to place the issue in the broader legal context. Defendants have the obligation to protect Georgia citizens’ constitutional right to vote and have the further obligation to ensure that the votes are counted and recorded accurately. Plaintiffs have shown that DRE machines, particularly in Georgia, cannot be relied upon to protect these vital constitutional rights; their continued use, therefore, is not a constitutional option, any more than it is an option for the state to maintain segregated schools because busing is difficult, *Swan, supra*, or to maintain inhumane prison conditions because building enough prisons is not in the budget, *Brown, supra*.

As a factual matter, however, replacing DRE machines with paper ballots for the 2018 election is completely feasible and practical.

1. *Proposed Remedy – Paper Ballots*

a) *Step-by-step description*¹⁴

Defendants exaggerate the difficulty of injunctive relief by exaggerating the scope and nature of the Coalition Plaintiffs' proposed remedy. To explain the limited scope of changes that the Coalition Plaintiffs seek for the 2018 election, the Coalition Plaintiffs have attached two charts as demonstrative Exhibits F and G. Exhibit F shows the basic components of Georgia election system currently being used and if the injunction were granted. Exhibit G shows each of the steps of the voting process, both under the current system for in-person voting, under the current system for provisional voting¹⁵ at a polling place, and under the proposed polling place paper ballot system that would be used if the preliminary injunction were granted.

As Exhibit G shows, because paper ballots are already used in Georgia for provisional ballots, the proposed paper ballot system does not introduce any new steps in the voting process:

*Step One: The Diebold DRE system electronic poll book, which is used to verify voters' registration information and to select the correct ballot for each

¹⁴ Defendants feign confusion and uncertainty over the nature of the Coalition Plaintiffs' proposed remedy, but every step of the proposed remedy, including the various statutory options for scanning paper ballots, is described in detail in Coalition Plaintiffs' counsel's letter to the State Defendants' counsel dated April 16, 2018. (Doc. 258-1, pages 92, 93, and 96-97).

¹⁵ Provisional voting is more complex than the chart shows. No change is sought as to how provisional ballots are processed.

voter, would continue to be used, with pre-election corrections of discrepancies and a paper back up of the pollbook recommended (*see* Section A(2), below).

*Step Two: Currently, the voter is given a DRE voter access card *or*, if he or she is a provisional voter, a paper ballot. Under the proposed paper ballot system, all voters will be given a paper ballot, not a DRE voter access card.

*Step Three: Currently, (a) the voter inserts the DRE voter access card into the DRE machine and casts his or her votes by using the touchscreen or (b) if the voter is a provisional voter, he or she will mark the paper ballot and place it in a secure ballot box (inside a provisional voter envelope). Under the proposed paper ballot system, all voters will mark the paper ballot and place it in a secure ballot box. (Only provisional voters would use envelopes and provisional ballot paperwork.)

Step Four through Six: Currently, (a) votes from DRE machines are transmitted by memory cards to the GEMS server which tabulates voting results and (b) provisional voters' votes (once verified) are transmitted to the GEMS server via an Accuvote Optical Scanner memory card. Under the proposed paper ballot system, all ballots are transmitted to to the GEMS server via an Accuvote Optical Scanner memory card.

b) *Paper ballots are already authorized by statute*

Paper ballots have been an authorized form of voting under Georgia law continuously for over 240 years. (Article IX Georgia Constitution of 1777). Paperless mechanical lever voting machines were first permitted in approximately 1930 and optical scanners were authorized for the counting of paper ballots by 1981. (*See* O.C.G.A. §§ 21-2-280). DRE machines were first permitted in 2002. Ga. L. 2002, p. 598; Ga. L. 2003, p. 517. None of these laws authorizing mechanical or electronic voting systems, however, required their use or supplanted the authority to use hand-counted or electronically counted paper ballots.¹⁶

O.C.G.A. § 21-2-379.3 permitted Georgia's first use of DRE voting systems in 2002 and required that the Secretary of State provide DRE equipment to all counties, after funds were appropriated by the General Assembly. The law, however, does not mandate their use. In fact, the State provided both DREs and optical scanning equipment for paper ballots. Further, counties retain the statutory authority to use optical scanning equipment to scan and count paper ballots, and absentee mail-in and provisional ballots.

In addition, under O.C.G.A. § 21-2-379.2, the Secretary has the authority to revoke his approval of a DRE voting system if he re-examines the system and

¹⁶ Indeed, numerous Georgia statutes authorize, require or contemplate the use of paper ballots today. *See, e.g.*, O.C.G.A. § 21-2-280; § 21-2-281; § 21-2-366; and § 21-2-4-483.

determines that it “can no longer be safely or accurately used by electors at primaries or elections . . . because of any problem concerning its ability to accurately record or tabulate votes.” The evidence in this case compels such a finding and a wholesale revocation of Georgia’s DREs. However, given the underlying statutory authority to use paper ballots (either hand-counted or counted by optical scan equipment), and the absence of any state law requiring use of DREs, the replacement of the DREs in lieu of paper ballots does not require the Secretary to invoke O.C.G.A. § 21-2-379.2.

The Coalition Plaintiffs do not agree that a change to all-absentee mail-in balloting is an appropriate solution to insecurity of DREs. The State Defendants raise a number of objections to an all-mail-ballot solution. In response, the Coalition Plaintiffs note simply that none of those objections apply to a simple substitution of paper-ballot voting, with optical scan counting, in place of DRE voting. As discussed above, Georgia law already allows and provides for paper ballot voting and optical-scan counting. Moving the State to all-absentee mail balloting, by contrast, would require adoption of an entirely new statutory and regulatory regime. Moreover, there is ample evidence that absentee ballots entail their own injury to voters, not least among which is the risk of the voter’s complete disenfranchisement in the event of a signature mismatch (a judgment call by officials) or an erroneously filled out mail-in envelope(an innocent mistake by the

voter). Paper ballots suffer from none of the collateral problems and thus are the clearly preferable solution and the only one authorized by state law, among the options presently before this Court.

c) Availability of additional paper ballots

Paper ballots and printing capacity are available at prices less than quoted by Defendants. (Martin Declaration, attached hereto as Exhibit D, ¶¶34-39, 46.)

d) Optical scanners

A repeated theme in the declarations submitted by the Defendants is that the paper ballots will be too difficult to scan: the optical scanners are too slow, will overheat, or are unavailable. To the contrary: Defendants have three different feasible, time tested options authorized by statute for counting paper ballots: (1) scanning the paper ballots in each polling place, which is the most commonly used ballot scanning configured nationwide; (2) scanning the paper ballots in a central location in each county, which is done in every county for mail and provisional ballots; or (3) hand counting the paper ballots, which is done today in several small Georgia municipalities.

For most counties, scanning the paper ballots in a central location – the second option - will be the easiest, and deploying this remedy eliminates the vast majority of objections and concerns raised in the declarations filed by Defendants. However, Coalition Plaintiffs, consistent with their April 16, 2018 letter to

Defendants' counsel (Doc. 258-1, pages 92, 93, and 96-97), recognize that current statutes permit each county to make its choice locally among these three options, dependant on its needs and resources, and do not request that any one of the three authorized methods be selected as a uniform election method.

The State Defendants argue that optical scanners can play no part in any remedy fashioned by this Court because scanners, like DREs, are computers that can likewise be infected with malware. (Doc. 265, at 15–16, n.5.) This is a disingenuous objection because it ignores the solution already offered by the Coalition Plaintiffs—pre-certification audits of the election results, (Doc. 258-2, at 2, ¶ 4.) with federal funding available for implementation.¹⁷

All computerized systems are vulnerable to hacking and errors, but only the use of paperless DREs makes election results unverifiable and errors encountered irreversible. Paperless DREs record votes without creating any artifact of the voters' selections that can be used to verify the results reported by the DRE. Scanners do not suffer from this problem because they count votes that voters record on paper, and thereafter the voter-marked paper ballots remain available to

¹⁷ Since March 18, 2018, the U.S. Election Assistance Commission has made \$380 million of federal grant funds available to Georgia and other States to pay to, among other things, “[i]mplement a post-election audit system that provides a high level of confidence in the accuracy of the final vote tally.” See EAC, *2018 HAVA Election Security Funds*, <https://www.eac.gov/2018-hava-election-security-funds/#how-can-states-use-the-funds> (last visited Aug. 19, 2018). Georgia's share of these federal grant funds is \$10,305,783. See EAC, *2018 HAVA Election Security Grants*, https://www.eac.gov/assets/1/6/2018_HAVA_Election_Security_Funds.pdf (last visited Aug. 19, 2018).

be audited to verify the totals reported by the scanners. Performing audits of the scanner totals—prior to certification of election results—is exactly what Coalition Plaintiffs have proposed both to this Court and to the Defendants directly. (Doc. 258-2, at 2, ¶ 4 (proposed injunction); Doc. 226, at 72, ¶ C (Third Amended Compl. prayer); Doc. 258-1, at 95–98 & at 97 (Apr. 16, 2018, letter to Defendants’ counsel) (“It is also imperative that robust post-election audits of the unofficial results be completed before the election results are certified.”).)

Defendants suggest that because of the asserted insecurity of scanners, a timeconsuming statewide hand count of paper ballots is the only solution that can avoid the flaws of the DRE system. This is not true. Scanners are not necessary to the requested relief, but they do allow for faster, practical, and more accurate counting of paper ballots in a fashion currently authorized by Georgia statute. The use of paper ballots, optical scanners, and pre-certification audits together permits any manipulation of the election results to be detected and addressed, while also ensuring that election results can still be generated and reported as quickly as the public expects.

As noted above, counties may continue to do what they do now with provisional paper ballots: transport them in secure ballot boxes to the election office for central scanning and tabulation, along with the mail ballots. Election

office central count staff know how to use these scanners, and will be using them whether or not this relief is granted.

2. Proposed Remedy – Verification of Accuracy of Electronic Pollbooks

The Coalition Plaintiffs are also seeking injunctive relief relating to the electronic pollbooks. This aspect of the Plaintiffs' Motion has become increasingly important since the filing of the Motion because of the number of reported discrepancies in recent elections – discrepancies not addressed by Defendants in their Response. In addition, the State Defendants, in their Response, confirm (by their silence) that they have done nothing since the KSU-hosted statewide election system was exposed in 2016 to 2017 to verify the security of this essential database.

Therefore, as stated in the Motion for Preliminary Injunction, the Coalition Plaintiffs are seeking an order directing the Secretary of State, “before October 1, 2018, to conduct an audit of and correct any identified errors in the DRE system’s electronic pollbook data that will be used in both such elections.” (Doc. 258, page 2). The audit function, which may require external consulting resources given the urgency, should focus on assuring that all changes made to voter records in the last three years were authorized and properly recorded. The audit should assure that electronic pollbook voter data is consistent with the official voter registration data.

The purpose of this audit is to avoid voter disenfranchisement, confusion and incorrect ballot issuance in the upcoming election.

At a minimum, after discrepancies are corrected, current paper backup copies of the pollbooks must be printed after early voting and maintained at the polling places.

3. *Significant cost savings and federal funding*

Plaintiffs presented evidence with the opening Brief explaining how difficult and time consuming it is to conduct elections using DRE machines, which are difficulties and costs that will be avoided if injunctive relief is granted. In their Response, Defendants complain about the added cost of the proposed remedy, but do not subtract the enormous savings that will result from not having to program, test, transport and secure each of the Secretary's 27,000 DRE machines and associated memory cards before and after the elections. In addition,

C. Defendants' Other Arguments are Without Merit

Defendants make a number of other miscellaneous defensive arguments, none with any merit:

1. *Absentee Voting is Not a Constitutionally Adequate Alternative Remedy*

The State Defendants and Fulton County argue that there is no legal authority holding that the right to vote is burdened by the voter being forced to choose between voting in person on a DRE and voting an absentee mail-in paper

ballot. (Doc. 265, at 32–33 & n.14; Doc. 267, at 4–5.) This argument is wrong for three reasons.

First, the citizen’s right to vote and have their vote counted necessarily includes the right to have *all* votes counted correctly. *United States v. Saylor*, 322 U.S. 385, 386 (1944). Thus, if DRE machines are used at all in the election, a citizen’s right to have their voted counted correctly is still infringed even if he or she uses absentee ballots.

Second, mail-in absentee ballot entails costs, risks of disenfranchisement, and inconveniences exactly like other burdens that the Eleventh Circuit has held to infringe upon the right to vote. For example, mail-in absentee voters are subjected to signature verification that has no cure process, *see* O.C.G.A. § 21-2-386(a)(1), which exposes voters to a risk of being erroneously disenfranchised. This mail ballot disenfranchisement is currently occurring in Georgia at alarming levels.¹⁸ Voters suffer cognizable injuries by being exposed to the risk of erroneous disenfranchisement, *Arcia v. Florida Secretary of State*, 772 F.3d 1335, 1342 (11th Cir. 2014), having to pay postage or being “required to make a special trip to the county registrar’s office,” *Common Cause/Georgia v. Billups*, 554 F.3d 1340, 1351 (11th Cir. 2009), or being unable to vote in person in the voter’s home precinct. *Charles H. Wesley Educ. Found., Inc. v. Cox*, 408 F.3d 1349, 1352 (11th Cir.

¹⁸ Second D. Bowers Decl., attached hereto as Exhibit B, ¶¶ 9-10.

2005). Voting by mail-in absentee ballot plainly burdens the right to vote that in ways that are additional to the burdens of voting in person at the polls.

Third, the unconstitutional conditions doctrine prohibits the State from “condition[ing] receipt of a benefit or privilege on the relinquishment of a constitutional right.” *Bourgeois v. Peters*, 387 F.3d 1303, 1324 (11th Cir. 2004).¹⁹ The Eleventh Circuit “has roundly condemned the use of unconstitutional conditions” and held in *Bourgeois* that “an especially malignant unconstitutional condition” is presented where “citizens are being required to surrender a constitutional right ... not merely to receive a discretionary benefit but to exercise [] other fundamental rights.” *Id.*

The Defendants argue that Georgia voters are not constitutionally burdened by the requirement to use DREs for in-person voting because voters may still vote by “voluntarily” abandoning their ability to cast a ballot in person at their precinct on Election Day and suffering the burdens of mail-in absentee voting. Exactly this kind of choice was rejected in *Bourgeois* in the context of the First Amendment. *See* 387 F.3d at 1324–25 (“The ability of protestors to avoid the searches by declining to participate in the protest does not alleviate the constitutional infirmity of the City's search policy[.] ... [T]he existence of other vehicles through which

¹⁹ The Third Amended Complaint pleads violation of the unconstitutional conditions doctrine as grounds for relief with respect to both Counts. (Doc. 266, at 5, ¶ 2; at 62–63, ¶ 158; at 65, ¶ 162 (last bullet); at 67, ¶ 173 (Count I); at 70, ¶ 181 (Count II).)

protestors could voice their disagreement ... does not in any way alleviate the unconstitutional conditions problem.”)²⁰ Here, as in *Bourgeois*, the State may not excuse its unconstitutional burdening of in-person voting (through the DRE requirement) by suggesting that voters can simply avoid that unconstitutional burden by choosing to use a different, more onerous voting method instead. Such a “choice” is not a *defense* to constitutional violations, but is rather a constitutional violation by itself.

2. *Effective relief may be granted against these Defendants.*

The State Defendants challenge redressability on grounds that any injunction prohibiting the use of DREs to conduct in-person voting will not operate directly against the 158 counties of Georgia that are not parties to this case, and because the State Defendants lack authority to enforce counties’ compliance with such a prohibition. (Doc. 265, at 15, n.4.) This objection is untenable for several reasons.

First, the State Defendants’ objection that they lack authority to enforce counties’ compliance with this Court’s injunction against requiring in-person

²⁰Defendants rely upon *Favorito v. Handel*, 295 Ga. 795 (2009). The Georgia Supreme Court’s holding in *Favorito* was explicitly based on the factual finding that DRE machines were as secure and reliable as paper ballots, a finding that is inconsistent with all of the evidence in this case. Based on this now-obsolete factual finding, the Georgia Supreme Court held that requiring voters to use DRE machines or absentee ballots did not violate voters’ right to vote. The Georgia Supreme Court had no occasion to consider the facts of this case, in which voters are being forced to choose between DRE machines which are *not* secure or absentee ballots. Under Eleventh Circuit precedent, a state may not constitutionally force that kind of choice.

voters to use DREs can be addressed conclusively by simply including in the injunction a requirement that the Secretary revoke his approval of the DRE component of Georgia's voting system. Immediate revocation of this approval is mandated by O.C.G.A. § 21-2-379.2(c) in the event of a finding—which may be made by this Court with binding effect upon the Secretary—that the DRE system “can no longer be safely or accurately used by electors.” Once the Secretary has revoked his approval of the DRE system, DREs may not lawfully be used in any Georgia elections. *See* O.C.G.A. § 21-2-379.2(c).

Second, the State Defendants persist in arguing that O.C.G.A. § 21-2-383(b) somehow independently requires the use of DREs. The plain language of the statute itself refutes this misrepresentation. The statute only applies to absentee in-person voters, and it only requires these voters to use DREs *if* DREs “are used at the polling places on election day.” O.C.G.A. § 21-2-383(b). Apart from SEB Rule 183–1–12–.01, (which conflicts with controlling statutes), nothing in Georgia law requires that DREs must be used in polling places on Election Day, and O.C.G.A §21-2-366 specifically authorizes the use of optical scanners. Therefore, if the Defendants are enjoined from enforcing the SEB Rule, there is no other requirement in Georgia law that mandates the use of DREs by any voters at all. Of course, “state policy must give way when it operates to hinder vindication of

federal constitutional guarantees.” *Missouri v. Jenkins*, 495 U.S. 33, 50 (1990) (citations omitted).

Third, Article III standing requires that there be a “substantial likelihood that the judicial relief requested will prevent or redress the injury.” *Duke Power Co. v. Carolina Environmental Study Group, Inc.*, 438 U.S. 59, 74–75 & n.20 (1978). The Coalition Plaintiffs will clearly obtain some individual relief as a result of an injunction entered against the Secretary and Fulton County, *regardless* of whether other counties in Georgia are likewise enjoined. Such “partial relief is sufficient for standing purposes[.]” *Made in the USA Found. v. United States*, 242 F.3d 1300, 1310 (11th Cir. 2001) (quoting *Swan v. Clinton*, 100 F.3d 973, 981 (D.C. Cir. 1996)).

Finally, the Defendants are mistaken to assume that injunctive relief against the Secretary and State Board Members will not accrue to the benefit of all Georgia’s voters. Once this Court has ruled it unconstitutional for Fulton County to require in-person voters to use DREs under SEB Rule 183–1–12–.01, it is substantially likely that other county officials across Georgia, facing these identical facts, will voluntarily conform their conduct to the terms of the injunction.²¹ The common-law judicial presumption is that government—including county

²¹ Counties that have already been exploring ways to switch to paper ballots, only to be dissuaded by the Secretary (*see* Doc. 258-1, page 102) are especially likely to conform their conduct to the requirements of the injunction.

governments—will act lawfully. *See FCC v. Schreiber*, 381 U.S. 279, 296 (1965). *Cf. Int’l Union v. Brock*, 477 U.S. 274, 291–93 (1986) (rejecting similar redressability argument based on non-joinder “of every state agency whose cooperation was needed to effect the relief granted”).

3. *The laches defense does not apply*

Defendants’ argument²² that Plaintiffs’ motion is barred by the doctrine of laches is without merit for a number of reasons. “This defense ‘requires proof of (1) lack of diligence by the party against whom the defense is asserted, and (2) prejudice to the party asserting the defense.’ ” *Nat’l R.R. Passenger Corp. v. Morgan*, 536 U.S. 101, 121-22 (2002) (Thomas, J.) (citations omitted). Plaintiffs have been diligently seeking this exact remedy since they filed suit in 2017. It is true that the Court set an initial deadline of September 1, 2017, to seek a preliminary injunction, but that was to enjoin the use of DRE machines in the November 2017 election. More recently, counsel for Coalition Plaintiffs stated in open court on May 1, 2018, that Plaintiffs were looking for preliminary injunctive relief for the November 6, 2018 election, and anticipated filing a motion in mid-July. Plaintiffs’ motion was filed on August 3, 2018, and the Court’s modestly accelerated briefing schedule has kept the matter on its anticipated track. (*See* May 1, 2018 Tr. at 25-26).

²² (Doc. 267, pages 6 – 8; Doc. 265, pages 14-17).

Plaintiffs did not bring this motion earlier because Defendants' filing of a frivolous sovereign immunity defense blocked discovery. By July, however, the warnings from the federal government and cybersecurity experts had reached such a serious level, and escalating numbers of DRE system malfunctions, were being communicated to Coalition Plaintiffs, that Coalition Plaintiffs realized (a) Coalition Plaintiffs did not need discovery to prove their claims and (b) seeking immediate relief to address escalating malfunctions and this "national security concern" had become imperative.

Moreover, though Defendants complain about the burden of the injunctive relief generally (addressed above), Defendants do not identify any prejudice caused by the timing of the filing of the motion. *Morgan, supra*. Specifically, Defendants do not identify any material action that would have to be undone if the motion is granted – the deployment of the DRE machines has not begun. In addition, Defendants do not identify any actions that need to be taken now that would not have been necessary had the motion been filed earlier. More paper ballots and scanners (if actually needed) may be ordered in the ordinary course of preparing for the election.

The cases that Defendants cite in support of their laches argument are easily distinguishable on their facts, *e.g. Miller v. Bd. Of Com'rs of Miller County*, 45 F. Supp. 2d 1369, 1373 (M.D.Ga. 1998) (several year delay and an extraordinary

remedy proposed two weeks prior to election); or support the rejection of the defense. *United States v. Barfield*, 396 F. 3d 1144, 1150 (11th Cir. 2005) (death penalty case, rejecting laches defense because defendant “ha[d] not demonstrated she suffered undue prejudice from the delay”).

4. *Old cases about DRE machines are not relevant.*

Defendants cite several cases from other jurisdictions turning away challenges to DRE machines. *E.g. Weber v. Shelley*, 347 F.3d 1101 (9th Cir. 2003); *Schade v. Maryland State Bd. of Elections*, 401 Md. 1 (2007); *Andrade v. NAACP*, 345 S.W.3d 1 (Tex. 2011). Each of these, however, was decided without the full benefit of the conclusions of the entire computer science and national security communities to the effect that the machines are unreliable and must be replaced, and did not involve the unique circumstances presented by the exposure of the entire state system to potential access by malicious users under Secretary Kemp’s watch.

5. *Mandatory preliminary injunctive relief is appropriate.*

Citing Georgia appellate caselaw which does not govern this federal question case in federal court, the Fulton County defendants argue that preliminary injunctive relief is limited to maintaining the status quo. (Doc. 267, page 5). This is not the law. In *Canal Authority v. Callaway*, 489 F.2d 567, 576 (5th Cir. 1974), the Former Fifth Circuit recognized that it is “often loosely stated that the purpose

of a preliminary injunction is to preserve the status quo.” The court continued: “It must not be thought, however, that there is any particular magic in the phrase ‘status quo.’”

If the currently existing status quo itself is causing one of the parties irreparable injury, it is necessary to alter the situation so as to prevent the injury . . . by the issuance of a mandatory injunction, see 7 Moore's Federal Practice P65.04(1), or by allowing the parties to take proposed action that the court finds will minimize the irreparable injury. The focus always must be on prevention of injury by a proper order, not merely on preservation of the status quo.

Id. Here, an order enjoining the use of DRE voting machines in the upcoming elections is necessary to prevent irreparable injury and is therefore the appropriate remedy.

III. Conclusion

In sum, the Coalition Plaintiffs have met their burden for the granting of preliminary injunctive relief under *Winter v. NRDC*, 555 U.S. 7, 20 (2008), and their Motion for Preliminary Injunction should be granted.

This 20th day of August, 2018.

/s/ Bruce P. Brown

Bruce P. Brown
Georgia Bar No. 064460
BRUCE P. BROWN LAW LLC
Attorney for Coalition for
Good Governance
1123 Zonolite Rd. NE
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

/s/ Robert A. McGuire, III

Robert A. McGuire, III
Admitted Pro Hac Vice
(ECF No. 125)
Attorney for Coalition
for Good Governance
Robert McGuire Law Firm
113 Cherry St. #86685
Seattle, Washington 98104-2205
(253) 267-8530

/s/ William Brent Ney

William Brent Ney
Georgia Bar No. 542519
Attorney for Coalition
for Good Governance, William
Digges III, Laura Digges, Ricardo
Davis, and Megan Missett
Ney Hoffecker Peacock & Hayle,
LLC
1360 Peachtree Street NE
Atlanta, Georgia 30309
(404) 842-7232

/s/ Cary Ichter

CARY ICHTER
Georgia Bar No. 382515
Attorney for William Digges III, Laura
Digges, Ricardo Davis and Megan Missett
Ichter Davis LLC
3340 Peachtree Road NE
Suite 1530
Atlanta, Georgia 30326
(404) 869-7600

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRIAN KEMP, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing document has been prepared in accordance with the font type and margin requirements of LR 5.1, using font type of Times New Roman and a point size of 14.

/s/ Bruce P. Brown

Bruce P. Brown
Georgia Bar No. 064460
BRUCE P. BROWN LAW LLC
Attorney for Coalition for
Good Governance
1123 Zonolite Rd. NE
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRIAN KEMP, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

CERTIFICATE OF SERVICE

This is to certify that I have this day caused the foregoing COALITION PLAINTIFFS' REPLY BRIEF IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION to be served upon all other parties in this action by via electronic delivery using the PACER-ECF system.

This 20TH day of August, 2018.

/s/ Bruce P. Brown
Bruce P. Brown
Georgia Bar No. 064460
BRUCE P. BROWN LAW LLC
Attorney for Coalition for
Good Governance
1123 Zonolite Rd. NE
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

E
X
H
I
B
I
T

A

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

DONNA CURLING, ET AL.,
Plaintiffs,
v.
BRIAN KEMP, ET AL.,
Defendants.

Civil Action No. 1:17-CV-2989-AT

SECOND DECLARATION OF MATTHEW D. BERNHARD

MATTHEW D. BERNHARD (“Declarant”) hereby declares as follows:

1. I incorporate all the statements made in my previous declaration given in this case on August 3, 2018, including exhibits thereto. (Doc. 258-1, at 33–42, 43–60.)

2. Georgia’s DRE voting machines are not sufficiently secure to have confidence that any election held in the state of Georgia adequately expresses the will of the people. As the voting machines produce no audit trail, and indeed the state performs no independent auditing at all, there is no way to verify that the result produced at the end of election night is correct. Furthermore, there can be no confidence that elections held prior to now have been correct or secure either, as

again any attempt to verify election returns is both impossible and prohibited by the Secretary of State.

3. As stated by the Secretary of State's CIO, (Beaver Decl., Doc. 265-1), the security of elections depends on much more than the voting mechanism. However, security cannot exist unless each component, including the voting mechanism, is independently secure. The chain of security is only as strong as its weakest link, and the chain of election security in Georgia is all but broken due entirely to the insecurity of Georgia's DRE voting machines.

4. The chain of custody of Georgia's voting machines is not properly maintained. Machines are left unattended in various public locations for days around election day. (Doc. 258-1, at 39-41, ¶¶ 34-40.) The security devices used to physically secure the machines are inadequate to ensure that no tampering has taken place. Last week at the DEF CON hacker conference in Las Vegas, I witnessed someone completely defeat a tamper-evident tie of the type used by Fulton County to secure DRE units in the field with nothing but a soda can. The "hacker" with only one day of experience in hacking tamper-evident seals was able to defeat the seal in less than 4 seconds. I also learned how to do this myself. By inserting a cut piece of aluminum into the ratchet mechanism of the ties, an attacker can undo the tie without breaking it, and then refasten the tie. Without near

microscopic examination, there is no evidence that the fastener has been tampered with. It takes mere minutes to learn how to do this. These are the fasteners that the state of Georgia relies upon to ensure attackers do not tamper with voting machines while left unattended, generally for days in the polling places. Thus, Georgia's DRE voting machines cannot be assumed to be tamper-free.

5. Because the software and hardware interfaces of DRE voting machines are so insecure, (Bernhard Decl., Doc. 258-1, at 34–39), physical security is the only mechanism by which the State of Georgia can hope to protect its DRE machines. Since the state cannot even physically secure its 27,000 voting machines and 30,000+ memory cards, it cannot guarantee that the machines tabulate votes accurately.

6. However, DREs are not the only inadequately secured part of Georgia's voting system, contrary to claims in (Beaver). Voter registration in Georgia can be changed online, with the service requiring name, date of birth, and county of residence. All of this information for nearly every voter in Georgia has already been leaked by the Center for Election Systems, as a server with this information was left wholly exposed on the Internet for months and possibly years. (Lamb Decl., Doc. 258-1, at 132, ¶ 20.)

7. I understand from news reports that electronic poll books have also been stolen and not recovered, and I am aware that the ExpressPoll units used in Georgia make no effort to encrypt the data that is stored on them, so an attacker could easily glean voter information and change registration this way as well.¹

8. The Secretary of State's CIO, Merritt Beaver, claims that the air gapped ballot building system is robust from external threats. (Beaver Decl., Doc. 265-1, at 3, ¶ 3.) An "air gap" typically means that the system in question is not connected to the Internet. However, as data changes from election to election, there must be a mechanism to update the ballot building system, likely a thumb drive or CD that was plugged into some other system that was connected to the Internet. If an attacker gets malware onto these components, they can get malware into the air gapped ballot building system, as was famously done in the case of the well-known Stuxnet exploit that used malware to damage the Iranian nuclear program and more recently exhibited in the "Industroyer" or "CrashOverRide" malware that has come to light that targets power grids. See The Hacker News, *Dangerous Malware Discovered That Can Take Down Electric Power Grids*,

¹ Jack Crosbie, *How a 16-Year-Old Hacked a Voting Machine This Weekend*, <https://www.inverse.com/article/34861-tj-horner-voting-machine-hack-defcon> (July 31, 2017) (last visited Aug. 20 2018).

<https://thehackernews.com/2017/06/electric-power-grid-malware.html> (June 12, 2017) (last visited Aug. 19, 2018).

9. Furthermore, even if the media used to transfer information is never plugged into a system that is exposed to the Internet by election officials, it could very well be the case that the manufacturer of the transfer media (e.g., USB sticks) could have placed malware on it before the state of Georgia came to possess it. The Chinese government is especially adept at doing this.²

10. As the Coalition Plaintiffs have pointed out, some of these attack vectors may indeed be “spectral fears,” but the point is not to claim that Georgia’s system has been hacked because of how many different entry points it has to hackers. Rather, the point is to highlight that no one can say with confidence that the system has *never* been hacked. And once it has been hacked, it is exceedingly difficult, if not impossible, to identify and eradicate whatever malware may have been installed and which thereafter can remain silently hidden. There is no external mechanism for verifying that votes in Georgia are tallied correctly. The Secretary of State’s CIO, Merritt Beaver, cites many security techniques employed by the Secretary to defend Georgia’s elections, all of which are commendable.

² Vojtech Bocek & Nikolaos Chrysaidos, *Android devices ship with pre-installed malware*, <https://blog.avast.com/android-devices-ship-with-pre-installed-malware> (May 24, 2018) (last visited Aug. 20, 2018).

However, these measures alone cannot guarantee that Georgia's elections are safe. When defending against hacking, you have to get it right every single time. When attacking, you only have to get it right once. Georgia has not and does not get it right every single time, and the State Defendants have offered no evidence to show that their negligence has not resulted in ongoing harm to Georgia voters. Even if the state wished to do so, Georgia's voting system provides no substantial evidence to support such a claim.

11. The only known robust mechanism for universally disclaiming election malfunction is a physical paper record.³ With paper ballots and a low-cost risk-limiting audit, we can gain confidence that none of the shortcomings of Georgia's election systems will impact the election results. Optical scanners by themselves, as pointed out by the Coalition Plaintiffs, are just as vulnerable as DREs. However, with a durable paper record of voter intent we can check afterward and know for sure whether the system has been hacked or has otherwise malfunctioned.

12. This argument similarly applies to voter rolls. Georgia is not a same-day-registration State, so there really is no need for voter registration data to be administered via computer in the polling place. A printed paper roster of voters

³ See Bernhard et al., "Public Evidence from Secret Ballots"
<https://mbernhard.com/papers/voting-sok17.pdf>

would be fine, and would also circumvent the need for vulnerable voter access cards and e-pollbooks.

Pursuant to 28 U.S.C. § 1746, I declare and verify under penalty of perjury that the foregoing is true and correct.

Executed on this date, August 20, 2018.

A handwritten signature in black ink, appearing to read "Matthew D. Bernhard", written over a horizontal line.

MATTHEW D. BERNHARD

E
X
H
I
B
I
T

B

**IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

DONNA CURLING, et al.

Plaintiff,

vs.

BRIAN P. KEMP, et al.

Defendant.

**CIVIL ACTION FILE NO.:
1:17-cv-2989-AT**

SECOND DECLARATION OF DANA BOWERS

DANA BOWERS hereby declares as follows:

1. I submitted a declaration in this lawsuit on August 3, 2018. This declaration supplements that information.
2. As stated in the previous declaration, I was required to vote a provisional ballot on July 24, 2018 at Gwinnett County Precinct 100 which is the precinct assigned to me on My Voter Page on the Secretary of State's website, although my home precinct is precinct 96.
3. I was assured by pollworkers at Precinct 100 that my ballot would count.
4. I received the letter dated July 31, 2018 from Gwinnett County attached in Exhibit 1. To my surprise, the letter states that my ballot was only partially counted because I voted in the incorrect precinct, although I

voted in the precinct assigned on Election Day on the Secretary of State official website, which I checked multiple times that day, and captured screenshots of the assignment to Precinct 100.

5. My experience of inaccurate polling place assignment and Diebold ExpressPoll electronic pollbook discrepancies is just one of many similar voting problems encountered by personal acquaintances in recent elections. I am increasingly concerned about whether the upcoming election can be fairly conducted with pervasive problems in the Diebold pollbook data and the Secretary's voter registration data.
6. As a member of the Josh McCall campaign, I am concerned about our voters being disenfranchised by the discrepancies in the voter records and pollbooks, including disenfranchisement such as I experienced in my vote not fully counting.
7. I stated in my August 3, 2018 declaration that I planned to vote by mail ballot and also undertake a campaign to promote mail in absentee ballots in order to increase the number of verifiable ballots in the election. However, upon studying the discouraging absentee mail ballot record status in my home county of Gwinnett, based on Secretary of State official records, I am reconsidering voting by mail or recommending voting by mail.

8. I have reviewed the absentee ballot status files for November 2016 and May 22, 2018 elections for Gwinnett County found on the Secretary of State's website at <http://elections.sos.ga.gov/Elections/voterabsenteefile.do>. I observed that hundreds of ballot applications and voted ballots have been routinely rejected for discrepant signatures or small clerical errors in completing the return ballot envelope. I particularly noticed a large number of elderly voters' signatures marked as not matching their voter registration files, and therefore rejected causing their ballot to be rejected.
9. I have learned that Georgia does not have a system to permit eligible mail ballot voters to cure signature discrepancies or other clerical mistakes such as including a birthdate on the return ballot envelope. A frequently reported error on the Secretary of State's worksheets is that voters write in the current date rather than their date of birth, and their ballot is rejected for that reason alone.
10. Voters are unaware that their ballot is being rejected until it is too late. Based on the very high numbers of rejections I reviewed, the risk of rejection and disenfranchisement is a meaningful risk and not one I want to encourage other voters to take.

11. I have not decided whether to attempt to vote by mail ballot and which balloting method carries the higher risk of disenfranchisement.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, August 20, 2018.

A handwritten signature in black ink, appearing to read 'DB', is written over a horizontal line.

Dana Bowers

EXHIBIT 1



455 Grayson Highway, Suite 200 • Lawrenceville, GA 30046-6388
(mailing/correo postal) 75 Langley Drive • Lawrenceville, GA 30046-6935
(tel) 678.226.7210 • (fax) 678.226.7209

July 31, 2018

DANA L BOWERS
3514 DEBBIE CT
DULUTH GA 30097

Registration Number: 05484692

DANA BOWERS,

This is official notification that your provisional ballot was partially counted for the July 24, 2018 General Primary and Special Election.

Because your ballot was cast in the wrong precinct, only the races for federal, state and countywide offices specific to your correct precinct were tabulated. Any other district races not specific to your correct precinct were not counted.

Your current Gwinnett County precinct is:

Precinct 096

Bunten Road Park

3180 Bunten Road

Duluth GA 30096

If you completed a registration application at the poll you should receive a new precinct identification card listing your precinct and district information. If you did not complete a registration application at the poll, but would like to register or update your information, you may complete an online application by going to www.mvp.sos.ga.gov.

If you have any questions regarding this issue, please contact this office. You may call 678.226.7210, Monday through Friday, from 8:00am until 5:00pm excluding holidays or email voterregistration@gwinnettcountry.com. If you choose to contact this office by email, you will need to include your full legal name in the email message.

Thank you for your interest in exercising your right to vote.

Sincerely,

Deputy Registrar
Gwinnett County Board of Registrations and Elections

gwinnettcountry

E
X
H
I
B
I
T
C

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRIAN KEMP, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

DECLARATION OF RICHARD A. DeMILLO

RICHARD A. DeMILLO (“Declarant”) hereby declares as follows:

1. I am a registered voter in Fulton County Georgia. I am deeply interested in the proper functioning of the Georgia’s voting system, from both a personal and professional perspective.
2. I am currently the Charlotte B. and Roger C. Warren Chair of Computer Science at Georgia Tech. I have served as Dean of the College of Computing at Georgia Tech and Director of the Georgia Tech Center for Information Security. I have also served as the Chief Technology Officer for Hewlett-Packard, Vice President and General Manager of Computing and Information Research at Bell Communications Research, Director of the Computer

and Communications Research Division at the National Science Foundation, and Director of the Software Test and Evaluation Project for the U.S. Department of Defense. In all these appointments, my primary technology focus has been information, communication, and cyber security and computer system testing. I have taught both graduate and undergraduate courses in cyber security, supervised graduate students, and conducted peer-reviewed research leading to journal articles, patents, and invited addresses, all related to the topic of cyber threats to computer systems.

3. A copy of my cv is attached as Exhibit 1.

4. I am familiar with Georgia's Diebold DRE voting system, its design, the body of academic literature compiled on the system in the last ten years, and its operation as it is deployed in the polling places in Georgia.

5. I own Diebold TSx and TS voting machines purchased over e-Bay which I have examined and used to conduct certain experiments related to the DRE system security. Over the past year, I have conferred with many colleagues in the field of cyber security, including Matthew Bernhard and Logan Lamb who have sought my technical input for their research into Georgia's DRE voting system.

6. I have observed the operation of the Diebold DRE system in polling places in multiple Georgia counties over the course of multiple elections and in county election offices where the system was being programmed and tested. I have

observed the testing procedures conducted prior to machine deployment to the polling places.

7. I have also observed the Diebold DRE voting machines being hacked in demonstrations, most recently in a public seminar at Georgia Tech in April 2018.

8. I am not a retained expert by any party to this action, but in the desire to aid the Court in the evaluation of the Defendant's assertions, I wish to voluntarily offer my opinion on one topic included in the State Defendant's response brief [Doc. 265, page 3]

9. In summary, Defendants' briefs and supporting declarations show a lack of basic understanding of the nature of current cybersecurity attacks being used against the nation's election systems and commercial systems. Defendants do not appear to understand the most basic realistic threats to the state's election system which may have already altered the operation of the system in undetected ways.

10. Defendants ridicule Coalition Plaintiffs, stating, "Undetectable manipulation' is Plaintiffs' phrase de jure for the convenient reason that it dodges any test for corroboration. Evidence of 'undetectable manipulation' is oxymoronic."

11. Defendants assert that Plaintiffs have concocted the idea of undetectable manipulation to suit the needs of the present lawsuit. This is a false assertion. Undetectable manipulation is the most common, widely recognized, and serious threat facing computer systems, including election systems. Techniques for undetectable manipulation, methods for counteracting the threats, and the capabilities that are needed to mount a successful defense to such attacks are defined by the National Institute of Standards and Technology (NIST) and are contained in the standard curriculum in virtually every university level course on cyber security. Furthermore, as the following citations show, the threat is not speculative or theoretical but rather is the fundamental building block of modern cyber security and cyber warfighting.

12. Undetectable manipulation is a standard behavior of Advanced Persistent Threats¹ or APT, the threats that the US Intelligence Agencies have determined with high confidence attacked US election systems in 2016 and continue to attack the mid-term elections². According to NIST, “The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of

¹ National Institute of Standards and Technology,
<https://csrc.nist.gov/Glossary/?term=2856>

² <https://www.burr.senate.gov/press/releases/senate-intel-committee-releases-unclassified-1st-installment-in-russia-report-updated-recommendations-on-election-security>

time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives."³ Attacks due to APTs are mounted by state and nonstate actors and constitute one of the principle attack vectors for modern cyberwarfare.⁴

13. There is ample publicly disclosed cause to believe⁵ that US election systems (including Georgia's) have been subject to APT attacks that yield undetectable manipulation. APTs use exactly the attacks that have been documented in classified and unclassified analyses of Russian activities⁶ to disrupt and hack US election systems⁷ "A persistent attack will probe networks, scour social networks for information they can find about the target's employee and perform other analysis and reconnaissance. Any organization that does not think they enough value to motivate a criminal to be persistent should be out of business."⁸

14. One characteristic of attacks mounted by APTs is that they can evade detection by doing damage before IT managers, antivirus companies, and

³ National Institute of Standards and Technology
<https://csrc.nist.gov/Glossary/?term=2856>

⁴ Jeffrey Carr, *Inside Cyberwarfare*, O'Reilly Publishers, 2009. P.119

⁵ <https://www.justice.gov/file/1080281/download>

⁶ *ibid*

⁷ <https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1>

⁸ Ira Winkler *APT Security*, p. 39

hardware/software vendors are aware that an attack has taken place: “If a virus can infect 10 million computers...in the hours before a fix is released, that’s a lot of damage. What if the code took pains to hide itself, so that a virus wasn’t discovered for a couple of days? What if [a] worm just targeted an individual, and deleted itself before off any computer whose userID didn’t match a certain reference?”⁹

15. Current textbooks on methods for subverting operating systems, answer these questions in great detail and should be well-known to election officials who operate the computer systems that are targeted by APTs: “A back door in a computer is a secret way to get access....They are very real...To remain undetected a back-door program must use stealth...Professional attack operations usually require specific and automated back door programs—programs that do only one thing and nothing else. This provides assurance of consistent results.”¹⁰ The software that installs these back-door programs and then erases all evidence of its existence is called a Rootkit.

16. There are catalogs of viruses and other programs that install Rootkits. These catalogs are studied by undergraduate computer science students to prepare

⁹ Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, 2000 p. 158

¹⁰ Greg Hoglund and James Butler, “Rootkits: Subverting the Windows Kernel,” Addison-Wesley, 2006 pp. 2–3

them to counter APTs in practice. Among these programs are Polymorphic Viruses: “These are the most difficult to detect. They have the ability to mutate, which means that they change the viral code known as the signature each time they spread or infect. Thus, antiviruses that look for specific virus codes are not able to detect such viruses.”¹¹

17. Standard textbooks¹² list the many forms that a back door might take:

a. “Install an altered version of *login*, *telnetd*, *ftpd*, *rshd*, *inetd*, or some other program; the altered program usually accepts a special input sequence¹³ and spawns a shell for the user.

b. Plant an entry in the *.rhosts*, *.shosts*, or *.ssh/authorized_keys* file of a user or the superuser to allow future unauthorized access.

c. Change the */etc/fstab* file on an NFS system to remove the *nosuid* designator, allowing a legitimate user to become *root* without authorization through a remote program.

¹¹ Ankit Fadia, “The Unofficial Guide to Ethical Hacking,” Premier Press, 2002 p. 434

¹² Simson Garfinkel, Gene Spafford, and Alan Schwartz, “Practical Unix & Internet Security (3rd edition), O’Reily Publishers, 2003

¹³ This capability is one of the reasons experts are alarmed by un-auditable bar codes in ballot marking devices. Such codes can embed such special input sequences.

- d. Add an alias to the mail system so that when mail is sent to that alias, the mailer runs a program of the attacker's designation, possibly creating an entry into the system.
- e. Change the owner of the */etc* directory so the attacker can rename and subvert files such as the */etc/passwd* and */etc/group* at a later time
- f. Change the file permissions of */dev/kmem* or your disk devices so they can be modified by someone other than *root*.
- g. Change a shared library or loadable module to add a system call option to allow a change to superuser status when using a seemingly innocuous program,
- h. Install a harmless-looking shell file somewhere that set SUID so a user can use the shell to become *root*.
- i. Change or add a network service to provide a *root* shell to a remote user.
- j. Add a back door to the *sshd* binary so that a specific username and password is always accepted for login, whether or not the username exists in the accounts database. Alternatively, the *sshd* binary might log all accepted usernames and passwords to a third-party machine.

Coupled with all of these changes, the attacker can modify timestamps, checksums, and audit programs so that the system administrator cannot detect the alteration!”¹⁴

18. Contrary to Defendants’ claims that hackers “usually leave footprints,” standard undergraduate cybersecurity textbooks describe how it is usual practice for APT attackers to cover their tracks and therefore not leave footprints:¹⁵ “After an attack succeeds, most attackers immediately cover their tracks. Log files are adjusted, hacking tools are hidden, and back doors are installed, making future re-invasions simple. Rootkit has a number of tools to do this, and many others are out there. All hackers have tools to hide their presence. The most common tool is *rm*, and it is used on *syslog*, *utmp*, *utmpx* files.”

19. Every computerized system in the Georgia Election System, including voter registration databases, employee and recruitment websites, network connected computers for provisioning systems of the kind located at the Kennesaw State University Center for Election Systems and which have now been transferred to the Office of the Secretary of State, Epollbooks used to provision voter cards on election day, servers used to provision ballot definitions on PCMCIA cards used in

¹⁴ Garfinkel et al p. 738–739

¹⁵ William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin, “Firewalls and Internet Security (Second Edition): Repelling the Wily Hacker,” Addison-Wesley Professional Computing Series, 2003, pp. 126–127

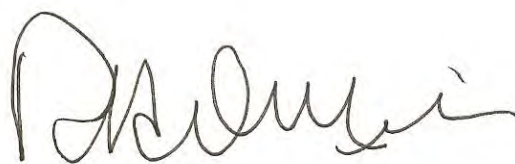
Diebold voting terminals, the voting terminals themselves, GEMS servers and related software for tallying election night results, optical scanners used to process absentee and provisional ballots, and election night reporting systems all contain operating systems that are susceptible to the attack described above. Contrary to Defendants' assertions direct Internet access is not required to mount such attacks.¹⁶

20. As these citations make clear, undetectable manipulation is a grave threat to Georgia's paperless DRE voting system because APTs have plainly targeted the American election system, including in all likelihood Georgia's system. It is well within the capabilities and consistent with usual practice of those APTs to utilize undetectable manipulation. Given the inability of the State to determine with any certainty whether the software presently being utilized by Georgia's DRE voting system has been maliciously altered at any point in the past, it will be impossible for Georgians to have any reasonable degree of confidence in the integrity of the election results produced by Georgia's DRE voting system.

¹⁶ Public demonstrations conducted by J. Alex Halderman in an open Seminar at Georgia Tech (April 16, 2018), witnessed by members of the public and legislative representatives from the Georgia House of Representatives and summarized for the general public in a New York Times article (<https://www.nytimes.com/2018/04/05/opinion/election-voting-machine-hacking-russians.html>). A written summary version of this experiment is being prepared for publication in technical journals.

Pursuant to 28 U.S.C. § 1746, I declare and verify under penalty of perjury that the foregoing is true and correct.

Executed on this date, August 20, 2018.

A handwritten signature in black ink, appearing to read "Richard A. DeMillo". The signature is written in a cursive, flowing style with a large initial "R".

RICHARD A. DeMILLO

EXHIBIT 1

Richard A. DeMillo

Curriculum Vita

Present Position

- Georgia Institute of Technology, Atlanta GA 30332
 - Charlotte B. and Roger C. Warren Professor of Computing
 - Professor of Management,
 - Executive Director, Center for 21st Century Universities

Education

- BA, Mathematics, 1969, College of St. Thomas, St. Paul Minnesota
- Ph.D., Information and Computer Science, 1972, Georgia Institute of Technology, Atlanta, Georgia

Professional Experience

2015-Present	Charlotte B. and Roger C. Warren Professor of Computing Executive Director, Center for 21 st Century Universities Georgia Institute of Technology Atlanta, GA 30332
2013-2014	Distinguished Chief Scientist Qatar Computing Research Institute Qatar Foundation Doha, Qatar
2002-Present (On Leave 2013-2014)	Professor of Management John P. Imlay Dean of Computing (2002-2009) Director, Georgia Tech Information Security Center (2002-2004) Georgia Institute of Technology Atlanta, Georgia 30332
2000-2002	Chief Technology Officer Vice President Hewlett-Packard Company 3000 Hanover Street Palo Alto, CA 94303
2000	General Manager Internet Systems Group Telcordia Technologies (Formerly Bellcore) 445 South Street Morristown, NJ 07960
1994-2000	Vice President and General Manager Information and Computer Sciences Research Telcordia Technologies (Formerly Bellcore) 445 South Street Morristown, NJ 07960
1994	Visiting Professor Department of Electronics and Informatics University of Padua Padua, Italy
1989-91	Director Computer and Computation Research Division National Science Foundation 1800 G Street NW

	Washington, DC
1987-96	Professor of Computer Science and Director Software Engineering Research Center Purdue University West Lafayette, Indiana
1985-87	Director Software Engineering Research Center Georgia Institute of Technology Atlanta, Georgia
1984-87	Assistant Director for Research School of Information and Computer Science Georgia Institute of Technology Atlanta, Georgia
1981-87	Professor of Information and Computer Science School of Information and Computer Science Georgia Institute of Technology Atlanta, Georgia
1976-81	Associate Professor of Information and Computer Science School of Information and Computer Science Georgia Institute of Technology Atlanta, Georgia
1972-76	Assistant Professor Department of Electrical Engineering and Computer Science University of Wisconsin, Milwaukee Milwaukee, Wisconsin
1969-72	Research and Teaching Assistant School of Information and Computer Science Georgia Institute of Technology Atlanta, Georgia
1969-71	Research Assistant Los Alamos National Laboratory Los Alamos, New Mexico

Research and Consulting Experience

Rich has been a consultant to many major corporations and other organizations. Detailed descriptions of recent consultantships are available upon request:

Board Memberships

Rich has been a board member and director of many public and private corporations, foundations and philanthropic organizations. Detailed descriptions of recent board memberships are available upon request:

Professional Recognition

ANAK, Outstanding Faculty Award (2106)

American Publishers Association Best Book Award (Education, 2016)

Inaugural Fellow of the Lumina Foundation

Fellow of the Association for Computing Machinery

Fellow of the American Association for the Advancement of Science

Panels and Advisory Positions

- 1983: Secretary of Defense Blue Ribbon Panel (The Eastman Panel) to Define the Software Engineering Institute (SEI)
- 1983-1985: IBM Software Tools Advisory Board
- 1984: Congressional Office of Technology Assessment Panel on Research Directions in Software Engineering.
- 1987: National Research Council Committee on Computer Security
- 1993-1996: National Research Council committee on Statistical Methods in Software Engineering
- 1992-1993: FAA VSCS Independent Fault Analysis Team
- 1995: National Research Council committee on Commercial Software Practices in Defense Software
- 1995-2000: Princeton University Computer Science Advisory Committee
- 1998-2000: Advisory Board of the College of Computing, Georgia Tech
- 2000-3: Georgia Tech Advisory Board
- 2001-2005: Advisory Board of the Johns Hopkins University Computer Sciences Department
- 2003-2005: National Research Council Committee on Telecommunications Research
- 2004-2005: National Research Council Committee on Network Science and the Army's Future Needs
- 2005 Defense Science Board Committee on Security of Software
- 2010-2013 Strategic Advisory Committee (Chair) Qatar Computing Research Institute
- 2012 AMA Advisory Board on Medical Education
- 2012-2016 World Economic Forum Global Action Council on the Future of Universities
- 2012-2015 Pacific Northwest National Laboratories National Security Advisory Council
- 2012-2016 Western Governors University Advisory Board
- 2013-2016 Singapore Institute of Technology and Design Advisory Board
- 2015 IEEE Computer Society, Research Advisory Board

Editorships

- 1990-96 Series Editor, *Software Science and Systems*, Plenum Publishing Company
- 1989-96 Editorial Board, *ACM Transactions on Software Engineering and Methods*
- 1988-94 Editorial Board, *IEEE Transactions on Software Engineering*
- 1985-87 Editorial Board, *Information and Control*
- 1982-85 Editorial Board, *ACM Transactions on Mathematical Software*

Biographical

- American Men and Women of Science
- Who's Who in America
- Who's Who in the World

Professional Societies

- Association for Computing Machinery
- American Mathematical Society
- Mathematical Association of America
- Society for Industrial and Applied Mathematics
- American Association for the Advancement of Science
- Association for Symbolic Logic
- IEEE

Rich has served on numerous program committees for professional meetings. In addition, Rich has served as Chairman or Program Chairman for the following annual conferences

- 15th International Conference on Software Engineering, 1993
- ACM SIGSOFT Annual Symposium, 1989 (Testing, Analysis and Verification)
- ACM Computer Science Conference, 1988
- ACM Symposium on Theory of Computing, 1984
- NSIA Conference on Test and Evaluation, 1983
- ACM Symposium on Principles of Programming Languages, 1982
- First IEEE Symposium on Security and Privacy, 1981

Publications

Books

- R. A. DeMillo, *An Education without Measure: Teaching and Learning the Science of Everyday Life, to be published 2019*
- R. A. DeMillo, *Revolution in Higher Education: How A Small Band of Innovators will Make College Accessible and Affordable*, MIT Press 2015 (foreword by Amb. Andrew J. Young)
- R. A. DeMillo, *Abelard to Apple: The Fate of American Colleges and Universities*, MIT Press, 2011.
- R. A. DeMillo and J. R. Rice, Editors, *Studies in Computer Science*, Plenum Press 1994
- R. A. DeMillo, W. M. McCracken, R. J. Martin, J. F. Passafiume, *Software Testing and Evaluation*, The Benjamin-Cummings Publishing Company, Inc. 1986.
- G. I. Davida, R. A. DeMillo, D. P. Dobkin, M. A. Harrison, R. J. Lipton, *Applied Cryptology, Cryptographic Protocols, and Computer Security*, American Mathematical Society (Applied Mathematics Series), 1984, American Mathematical Society. (Also: Indonesian edition, translated by Pangeran Sianipar, 1994)
- R. A. DeMillo, D. P. Dobkin, A. K. Jones, and R. J. Lipton, Editors, *Foundations of Secure Computation*, Academic Press, 1978

Special Publications

- "Statistics and Software Engineering", National Academy of Sciences, National Research Council Committee on Statistics, Document Number, 1996, Washington, DC.

- "Report of the Voice Switching and Control System (VSCS) Independent Fault Tolerance Analysis Team (VIFTAT)," A Report to the Federal Aviation Administration, MITRE Report (January, 1993).
- "Computer and Information Security in the Department of Energy's Classified Environment" (U), National Academy of Sciences, National Research Council Committee on Computer Security Doc. No. 88-EEB-2, 1988, Washington, DC (Classified Report)
- R. A. DeMillo, "Operational Readiness of the Patriot Air Defense System Software"(U), Report to Director Operational Test and Evaluation, USDRE, 1985 (Classified Report)
- R. A. DeMillo, "Software Test and Evaluation Manual: Volume 1, Guidelines for the Treatment of Software in Test and Evaluation Master Plans", Sept., 1984. Issued by the Office of the Secretary of Defense as Attachment to Department of Defense Directive 5000.3 ("Test and Evaluation") DoDD 5000.3-M-3.
- "Software Testing", *Encyclopedia of Information and Computer Science, 3rd Edition*, Anthony Ralston
- "Observing the 2006 Presidential Elections in Venezuela: Final Report of the Technical Mission," The Carter Center, 2007
- "New Ecosystems in Higher Education and What They Mean for Accreditation and Assessment, in WASC Concept Papers, 2nd Series: The Changing Ecology of Higher Education and its Impact on Accreditation, March 2013, Western Association of Schools and Colleges, Accrediting Commission for Senior Colleges and Universities.
- "Governance for a New Era: A Blueprint for Higher Education Trustees," Project on Governance for a New Era, Benno Schmidt, Chairman, August 2014
- "Deliberate Innovation, Lifetime Education: Report of the Commission on Creating the Next In Education," March, 2018. Georgia Tech

Recent Articles, Op-Ed and Opinion

"This Will Go On Your Permanent Record! How Blockchains Can Transform Colleges in a Networked World," The EvoLLLution, May 5, 2017, <https://evollution.com/programming/credentials/this-will-go-on-your-permanent-record-how-blockchains-can-transform-colleges-in-a-networked-world/>

"The Human Element and the Power of Big Data in Higher Education." The EvoLLLution, March 25, 2017

"Georgia's Election System Can't be Trusted." Bloomberg View, December 18, 2017, <https://www.bloomberg.com/view/articles/2017-12-18/georgia-s-election-system-can-t-be-trusted>

"Election Hacking is Going to Happen. Here's What We Can Do Now to Protect Our Vote," (with Candice Hoke and Duncan Buell) USA Today, March 25, 2018, <https://www.usatoday.com/story/opinion/2018/03/15/russian-election-hacking-what-we-can-do-now-protect-democracy-buell-demillo-hoke-column/393565002/>

"Gatekeepers No More: Colleges Must Learn a New Role," The Chronicle of Higher Education, September 14, 2015, <https://www.chronicle.com/article/Gatekeepers-No-More-Colleges/232975>

Patents

D. Boneh, R. DeMillo and R. Lipton, "Method of using transient faults to verify the security of a cryptosystem", Patent Number 6,965,673

Invited Talks, Keynotes

Rich is a frequent speaker at conferences and events. Details are available upon request

Papers and Book Chapters

1. J. Gough and R. A. DeMillo, "Towards an Ostensive Grammar I" *Eighth Annual Meeting of the Association for Computational Linguistics* (July 1970), Columbus, Ohio.
2. R. A. DeMillo, "An Application of an Ostensive Grammar to the Analysis of Existential Predicates", *Proceedings of the Southeastern Conference on Linguistics* (October 1970), Atlanta, Georgia.
3. L. Chiaraviglio and R. A. DeMillo, "On the Applicative Nature of Assignment", Georgia Institute of Technology Report Number GIT-ICS-71-1 (1971).
4. R. A. DeMillo, *Formal Semantics and the Logical Structure of Programming Languages*, Ph.D. Thesis, 1972, Georgia Institute of Technology, Atlanta, Georgia.
5. R. A. DeMillo, "Parallelism and Non-Determinism in the Lattice of Programs", *Record of the Computer Science Conference*, (February 1973), Columbus, Ohio.
6. R. A. DeMillo, "Constructing and Verifying Courses of Action in Robots," *Proceedings of MSAC-73*, (February 1973), Milwaukee, Wisconsin.
7. R. A. DeMillo and R. A. Northouse, "Autonomous Computing: Perspectives and Models for Artificial Intelligence," *Proceedings MSAC-74*, (February 1974), Milwaukee, Wisconsin.
8. R. A. DeMillo and K. Vairavan, "Parallel Scheduling of Programs in a Restricted Model of Computation", *Proceedings Sixth ACM Symposium on Theory of Computing*, (May 1974), Seattle, Washington.
9. R. A. DeMillo, "A Lattice Theoretic Interpretation of a Theorem by Patil," University of Wisconsin-Milwaukee Technical Report No. 75-6 (1975)
10. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "The Complexity of Control and Data Structures", *Proceedings Seventh Annual Symposium on Theory of Computing*, Albuquerque, New Mexico (May 1975), pp. 186-193.
11. R. A. DeMillo, S. Amoroso and M. Wolfe, "Primitives for Tactical Real-Time Control Languages based on Simula 67 II: Design and Implementation Considerations", CENTAC Report No. 58, US Army Electronics Command, Fort Monmouth, NJ (1975).
12. R. A. DeMillo, S. Amoroso and M. Wolfe, "Primitives for Tactical Real-Time Control Languages based on Simula 67 I: General Language Considerations", CENTAC Report No. 50, US Army Electronics Command, Fort Monmouth, NJ (1975).
13. R. A. DeMillo, "Nondefinability of Certain Semantic Properties of Programs", *Notre Dame Journal of Formal Logic*, Vol. 16, No. 4, (1975), pp. 583-590.
14. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "Space-Time Tradeoffs in Structured Programming", *Proceedings 1976 Johns Hopkins Conference on Information Systems and Sciences*, Baltimore, Maryland, (March, 1976), pp. 240-245.
15. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "Programming Language Studies I: The Power of Control and Data Structures" University of Wisconsin-Milwaukee Technical Report No. 76-13 (1976)
16. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "Can Structured Programs be Efficient", *SIGPLAN Notices*, Vol. 11, No. 10, (October, 1976), pp. 10-18.
17. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "Space and Time Hierarchies for Classes of Control and Data Structures", *Journal of the ACM*, Vol. 23, No. 4 (October, 1976), pp. 720-730.
18. R. A. DeMillo, S. C. Eisenstat, and R. J. Lipton, "Space-Time Tradeoffs in Structured Programming: Reducible Flowgraphs (Abstract Only), Computer Science Conference, 1976.
19. K. Vairavan and R. A. DeMillo, "On the Computational Complexity of a Generalized Scheduling Problem", *IEEE Transactions on Computers*, Vol. C-25, No. 10 (October, 1976), pp. 720-732. This paper has been reprinted under the same title in *Distributed Computing: Concepts and Implementations*, edited by Paul McEntire, John G. O'Reilly and Robert E. Larsen, published by IEEE Press (1984).
20. R. A. DeMillo, R. J. Lipton and A. J. Perlis, "Social Processes and Proofs of Theorems and Program", *6th ACM Symposium on Principles of Programming Languages* (January 1977) Santa Monica, California, pp. 245-262 [See main entry number [40] below].

21. R. A. DeMillo, K. Vairavan and E. Sycara-Cyranski, "A Study of Schedules as Models of Parallel Computation", *Journal of the ACM*, Vol. 24, No. 4 (October, 1977), pp. 544-565.
22. R. A. DeMillo, "Some Applications of Model Theory to the Metatheory of Program Schemata", *Notre Dame Journal of Formal Logic*", Vol. 18, No. 3, 1977, pp. 489-495.
23. R. A. DeMillo, S. C. Eisenstat, and R. J. Lipton, "Preserving Average Proximity in Arrays" *Communications of the ACM*", Vol. 23, No. 3, (March 1978), pp. 228-230.
24. R. A. DeMillo and R. J. Lipton, "A Constructive Generalization of the Borel-Cantelli Lemma with Applications to the Complexity of Infinite Strings", *Mathematical System Theory*", Vol, 13, 1979, pp. 95-104.
25. R. A. DeMillo, D. P. Dobkin and R. J. Lipton, "Combinatorial Inference", *Proceedings 1977 Allerton Conference on Communication, Control and Computing* [Also appears in R. DeMillo et al (editors), *Foundations of Secure Computation*, Academic Press, 1978, pp. 27-38.
26. R. A. DeMillo, D. P. Dobkin and R. J. Lipton, "Even Data Bases that Lie can be Compromised", *IEEE Transactions on Software Engineering*", Vol SE-4, No. 1 (January, 1978), pp. 71-74.
27. B. H. Barnes, G. I. Davida, R. A. DeMillo, L. H. Landweber, H. Stone, "Theory in the Computer Science and Engineering Curriculum", *IEEE Computer*", Vol. 18, No. 12 (December, 1977), pp. 106-108.
28. R. A. DeMillo, R. J. Lipton and L. G. McNeil, "Proprietary Software Protection" in R. A. DeMillo et al (editors), *Foundations of Secure Computation*", Academic Press, 1978, pp. 115-132.
29. R. A. DeMillo and D. P. Dobkin, "Foundations of Secure Computation", in R. A. DeMillo et al (editors), *Foundations of Secure Computation*", Academic Press, 1978, pp. 1-3.
30. R. A. DeMillo, S. C. Eisentat and R. J. Lipton, "On Small Universal Data Structures and Related Combinatorial Problems", *Proceedings 1978 Johns Hopkins Conference on Information Systems and Sciences*", March, 1978, Baltimore, Maryland, pp. 416-428.
31. R. A. DeMillo, R. J. Lipton and F. G. Sayward, "Program Mutation as a Tool for Managing Software Development", *Proceedings of the 32nd Annual Meeting of the American Society for Quality Control*", May 1978, Chicago, Illinois, pp. 326-348.
32. T. A. Budd, R. A. DeMillo, R. J. Lipton, and F. G. Sayward, "The Design of a Prototype Mutation System for Program Testing", *Proceedings 1978 National Computer Conference*", pp. 623-627.
33. R. A. DeMillo and R. J. Lipton, "A Probabilistic Remark on Algebraic Program Testing", *Information Processing Letters*, Vol. 7, No. 4 (June, 1978) pp. 193-195.
34. R. A. DeMillo, R. J. Lipton and F. G. Sayward, "Discussion of Software Testing Issues", in P. Wegner (editor) *Research Directions in Software Technology*", MIT Press (1978) pp. 408-413.
35. R. A. DeMillo, R. J. Lipton and F. G. Sayward, "Hints on Test Data Selection: Help for the Practicing Programmer", *Computer*, Vol. 11, No. 4 (April, 1978) pp. 34-43. This paper has been reprinted several times under the same title. It has recently appeared in Tutorial: *Software Testing and Validation Techniques* edited by Edward Miller and William Howden, IEEE Computer Society Press (1981).
36. R. A. DeMillo, R. J. Lipton and A. J. Perlis, "Response to Dijkstra's On a Political Pamphlet from the Middle Ages", *Software Engineering Notes*, Vol. 3, No. 2 (April, 1978) pp. 16-17.
37. R. A. DeMillo, R. J. Lipton and F. G. Sayward, "Program Mutation: A New Approach to Program Testing", in E. F. Miller (editor) *Software Testing, Volume 2: Invited Papers*, Infotech International, 1979, pp. 107-128. [Volume 1 on this work contains helpful analysis and bibliography].
38. R. A. DeMillo and R. E. Miller, "Implicit Computation by Synchronization Primitives", *Information Processing Letters*, Vol. 9, No. 1 (20 July 1979) pp. 35-38.
39. R. A. DeMillo and D. P. Dobkin, "Recent Progress in Secure Computation", *Proceedings 1978 IEEE COMPSAC* (November 1978) Chicago, Illinois.
40. R. A. DeMillo and R. J. Lipton, "Some Connections between Computational Complexity and Mathematical Logic", *Proceedings 11th ACM Symposium on Theory of Computing* (May 1979) Atlanta, Georgia, pp. 153-159.

41. R. A. DeMillo, R. J. Lipton and A. J. Perlis, "Social Processes and Proofs of Theorems and Program", *Communications of the ACM*, Vol. 22, No. 5 (May 1979) pp. 271-280. [See also correspondence in "ACM Forum", *Communications of the ACM*, vol. 22, No. 11 (November 1979); an earlier version of this paper was published in the proceedings of the 6th *ACM Symposium on Principles of Programming Languages* (January 1977) Santa Monica, California, pp. 245-262; This paper has been reprinted under the same title many times. It has appeared in *The Mathematical Intelligencer*, January, 1981, the 1984 anthology *Mathematics: People Problems, Results*, edited by D. C. Campbell and J. C. Higgins, published by Wadsworth International, the 1987 anthology *Currents in the Philosophy of Mathematics* edited by Thomas Tomaszko, the 1998 revised version which appeared under the title *New Directions in the Philosophy of* and the 1993 anthology *Program Verification*, edited by Timothy R. Colburn, James H. Fetzer and Terry L. Rankin, published by Kluwer Academic Publishers.
42. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "Space-Time Tradeoffs in Structured Programming: An Improved Combinatorial Embedding Theorem", *Journal of the ACM*, Vol. 27, No. 1 (January, 1980) pp. 123-127.
43. R. A. DeMillo and R. J. Lipton, "The Consistency of P=NP and Related Problems with Fragments of Number Theory", *Proceedings 12th ACM Symposium on Theory of Computing* (May 1980) Los Angeles, California, pp. 45-57.
44. R. A. DeMillo, "New Approaches to Program Testing", *IEEE Computer*, Vol. 12, No. 3 (March 1979) pp. 105-106.
45. R. A. DeMillo, "Data Base Security" in *Issues in Data Base Management*, H. Weber and A. Wasserman (eds.), North-Holland 1979, pp. 253-256.
46. R. A. DeMillo, R. J. Lipton and R. E. Miller, "Stochastic Synchronization," 1981 *Johns Hopkins Conference on Computer Systems and Sciences*, March 1981.
47. G. I. Davida, R. A. DeMillo, R. J. Lipton, "Sharing Cryptographic Keys," *Proceedings 1980 IEEE Symposium on Security and Privacy*, April 1980, Berkeley, California.
48. R. A. DeMillo and R. J. Lipton, "A System Architecture to Support A Verifiably Secure Multilevel Security System," *Proceedings 1980 IEEE Symposium on Security and Privacy*, April 1980, Berkeley, California.
49. T. A. Budd, R. A. DeMillo, R. J. Lipton and F. G. Sayward, "Theoretical and Empirical Results in Program Testing," *Proceedings Ninth ACM Symposium Principles of Programming Languages*, Las Vegas, Nev., January 1980, pp. 181-196.
50. R. A. DeMillo and F. G. Sayward, "Statistical Measures of Software Reliability," *Software Metrics*, edited by F.G. Sayward et al, MIT Press, 1981, pp. 185-202.
51. R. A. DeMillo and R. J. Lipton, "Software Project Forecasting," *Software Metrics*, edited by F.G. Sayward, et. al., MIT Press, 1981, pp. 77-94.
52. R. A. DeMillo, "Cryptographic Protocols," Presented at Meeting of American Mathematical Society, *Proceedings of Symposia in Applied Mathematics* (1981).
53. G. I. Davida, R. A. DeMillo and R. J. Lipton, "Achieving Secure Computers Through Distributed Computing", *Proceedings Third International Conference on Distributed Computing*, Paris, April 1981.
54. R. A. DeMillo, "Validating Computer Software: Two Views" *Transactions of the 1980 Annual Meeting of the American Nuclear Society*, Washington DC, November, 1980, pp. 251-252 (Invited Paper).
55. R. A. DeMillo, R. J. Lipton, and A. J. Perlis, "Social Processes and Proofs of Theorems and Programs," *The Mathematical Intelligencer*, January 1981. Reprinted. See main entry number [39]
56. R. A. DeMillo, N. A. Lynch, M. J. Merritt, "Cryptographic Protocols", *Proceedings, 14th ACM Symposium on Theory of Computing*, May, 1982, pp. 383-400.
57. R. A. DeMillo and M. J. Merritt, "Protocols for Data Security," *IEEE Computer*, Volume 16, Number 2, (February 1983), pp. 39-54

58. R. A. DeMillo and R. J. Martin, "Software Test and Evaluation Project: A Status Report", *NSIA National Conference on Software Test and Evaluation*, February 1-3, 1983, Washington, DC, pp. T1-T10
59. R. A. DeMillo, "Requirements for a Test and Evaluation Subenvironment of an Advanced Software Engineering Environment" Prepared by the Software Test and Evaluation Project, under Contract Number F33657-82-G-2083 to the Georgia Institute of Technology, Atlanta, Georgia 30332, April 1984
60. R. A. DeMillo, A. B. Marmor-Squires, S. T. Redwine, Jr., W. E. Riddle, "Software Engineering Environments for Mission Critical Applications - STARS Alternative Programmatic Approaches", IDA Paper #P-1788. Prepared for Office of the Under Secretary of Defense for Research and Engineering by Institute for Defense Analyses, August 1984
61. R. A. DeMillo, "Volume 2 - Software Test and Evaluation: State-of-the-Art Overview" OSD/DDT&E Software Test and Evaluation Project, Phases I and II, Final Report, submitted to the Office of the Secretary of Defense, Director Defense Test and Evaluation and the Office of the Naval Research ONR Contract Number N00014-79-C-0231, June 1983
62. R. A. DeMillo, R. J. Martin, "Volume 1 - Report and Recommendations" OSD/DDT&E Software Test and Evaluation Project, Phases I and II, Final Report, submitted to the Office of the Secretary of Defense, Director Defense Test and Evaluation and the Office of Naval Research ONR Contract Number N00014-79-C-0231, June 1983
63. K. Vairavan and R. A. DeMillo, "On the Computational Complexity of a Generalized Scheduling Problem," *Distributed Computing: Concepts and Implementations*, edited by Paul L. McEntire, John G. O'Reilly and Robert E. Larsen, published by the IEEE Press (1984). *Reprinted. See main entry number [18]*
64. R. A. DeMillo, R. A. Gagliano, R. J. Martin, and J. F. Passafiume, "Policy Recommendations for Software Test and Evaluation: System Level Test Issues", *Journal of Test and Evaluation*, January 1984, Vol. V, No. 1, pp 21-28
65. R. A. DeMillo, R. J. Lipton, and A. J. Perlis, "Social Processes and Proofs of Theorems and Programs," *Mathematics: People, Problems, Results*, edited by D. C. Campbell and J. C. Higgins, published by Wadsworth International (1984) *Reprinted. See main entry number [39]*
66. R. W. Bartlett and R. A. DeMillo, "Computer Litigation: What the Lawyer Expects and What the Expert Needs," *Computer Law: Institute of Legal Education*, July, 1986, Atlanta, GA, pp. 167-178.
67. R. A. DeMillo, "Functional Capabilities of a Test and Evaluation Subenvironment in an Advanced Software Engineering Environment" GIT-SERC-86/07.
68. R. A. DeMillo, E. H. Spafford, "The Mothra Software Testing Environment", *Proceedings 11th NASA Software Engineering Workshop*, NASA Goddard, December 3, 1986
69. E. W. Martin, R. A. DeMillo, "Operational Survivability in Gracefully Degrading Distributed Processing Systems," *IEEE Transactions on Software Engineering*, June 1986, Vol. SE-12, Number 2
70. R. A. DeMillo, et al "The Mothra Software Testing Environment System Documentation," Georgia Institute of Technology, Software Engineering Research Center, Atlanta, Georgia 30332, June 1987, GIT-SERC-87-10. (Second Revision published by The Software Engineering Research Center, Purdue University, January 1990)
71. R. A. DeMillo, D. S. Guindi, K. N. King & W. M. McCracken, "An Overview of the Mothra Software Testing Environment," Purdue University, Software Engineering Research Center, West Lafayette, Indiana 47907, August, 1987, SERC-TR-3-P
72. R. A. DeMillo, R. J. Lipton, and A. J. Perlis, "Social Processes and Proofs of Theorems and Programs," *Currents in the Philosophy of Mathematics* edited by Thomas Tomaszko (1987). *Reprinted. See main entry number [39]*
73. W. F. Applebee, R. A. DeMillo, D. S. Guindi, K. N. King, and W. M. McCracken, "Using Mutation Analysis for Testing Ada Programs," *Proceedings Spring 1988 Ada Europe Conference*, Munich, FDR. (North-Holland,

- 1988, also appears as Software Engineering Research Center, Purdue University Technical Report SERC-TR-9-P
74. B. Choi, R. DeMillo, W. Du, and R. Stansifer, "Observing Reusable Ada Software Components - Techniques for Recording and Using Operational Histories," Purdue University, Software Engineering Research Center, West Lafayette, Indiana 47907, 1988, SERC-TR-18-P
 75. R. A. DeMillo, D. S. Guindi, K. N. King, W. M. McCracken, and A. J. Offutt, "An Extended Overview of the Mothra Software Testing Environment," *Proceedings of the Second Workshop on Software Testing, Verification and Analysis*, Banff, Canada, July 1988, pp. 142-151
 76. R. A. DeMillo and A. J. Offutt, "Experimental Results of Automatic Test Data Generation," *Proceedings of Portland Software Quality Conference*, September 1988
 77. B. Choi, R. A. DeMillo, R. Stansifer, and W. Du, "Observation Packages for Reusable Ada Components," *Proceedings of Symposium on Empirical Foundations of Information Sciences and Systems* (October, 1988)
 78. R. A. DeMillo, E. W. Krauser and A. P. Mathur, "Using the Hypercube for Reliable Testing of Large Software," Software Engineering Research Center, Research Report Number SERC-TR-24-P, August, 1988, Purdue University
 79. H. Agrawal, R. DeMillo, and E. Spafford, "A Process State Model to Relate Testing and Debugging," Software Engineering Research Center, Research Report Number SERC-TR-27-P, September, 1988, Purdue University
 80. R. A. DeMillo, "Test Adequacy and Program Mutation," *Proceedings 1989 International Conference on Software Engineering*, May 1989, Also appears as Software Engineering Research Center, Research Report SERC-TR-37-P, Purdue University
 81. B. Choi, R. A. DeMillo, E. W. Krauser, R. J. Martin, A. P. Mathur, A. J. Offutt, E. H. Spafford, "The Mothra Toolset," *Proceedings 22nd HICSS*, January 1989
 82. R. A. DeMillo, "Software Testing for Critical Applications: A Position Paper," *Proceedings 13th IEEE Computer Software and Applications Conference*, Orlando, September, 1989, p. 521
 83. H. Agrawal, R. A. DeMillo, R. Hathaway, E. W. Krauser, R. J. Martin, and A. P. Mathur, "The Design of Mutation Operators for C", 1989 (Submitted for Publication), also appears as "Design of Mutant Operators for the C Programming Language", Software Engineering Research Center Research Report SERC-TR-41-P, Purdue University
 84. R. A. DeMillo and R. J. Lipton, "Software Windtunnels: Scale Models of Software Development Projects."
 85. H. Agrawal, B. Choi, R. A. DeMillo, and A. Mathur, "CIT/CAT: Two Novel Methodologies for the Design of Software Testing Tools," 1990
 86. R. A. DeMillo, E. W. Krauser, and A. P. Mathur, "An Approach to Compiler-Integrated Software Testing," Software Engineering Research Center, Research Report SERC-TR-71-P, April 1990, Purdue University
 87. H. Agrawal, R. A. DeMillo and E. H. Spafford, "An Execution Backtracking Approach to Program Debugging," *IEEE Software*, May 1991, p. 21-26
 88. R. A. DeMillo and R. J. Lipton, "Defining Software by Continuous, Smooth Functions," *IEEE Transactions on Software Engineering*, Vol. SE-17, No. 4, April 1991, p 383
 89. R. A. DeMillo, "Progress Toward Automating Software Testing," *Proceedings of the International Conference on Software Engineering*, Austin, Texas, May 1991, Also appears as Software Engineering Research Center Report Number SERC-TR-101-P, July, 1991, Purdue University
 90. Richard DeMillo and Aditya Mathur, "On the Use of Software Artifacts to Evaluate the Effectiveness of Mutation Analysis for Detecting Errors in Production Software," *Thirteenth Minnowbrook Workshop on Software Engineering*, (also Software Engineering Research Center Report Number SERC-TR-92-P, March, 1991, Purdue University)

91. R. A. DeMillo, E. W. Krauser, and A. P. Mathur, "An Overview of Compiler-Integrated Testing," *Proceedings of the 1991 Australian Software Engineering Conference*, Sydney, Australia, July 1991
92. R. A. DeMillo and A. J. Offutt, "Constraint-Based Test Data Generation," *IEEE Transactions on Software Engineering*, Vol. SE-17, Number 9, September, 1991, pp. 900-910
93. Hiralal Agrawal, Richard A DeMillo and Eugene H. Spafford, "Dynamic Slicing in the Presence of Pointers and Records," *Proceedings Fifth Symposium on Testing Analysis and Verification*, October, 1991, Victoria BC, pp. 60-73. (also appears as: Hiralal Agrawal and Richard DeMillo, "Dynamic Slicing in the Presence of Unconstrained Pointers," Software Engineering Research Center Report Number SERC-TR-93-P, March, 1991, Purdue University)
94. R. A. DeMillo, E. W. Krauser, and A. P. Mathur, "Compiler Support for Program Testing on MIMD Architecture," *Proceedings Ninth Annual Pacific Northwest Software Quality Conference*, October, 1991, Portland, Oregon
95. R. A. DeMillo and A. J. Offutt, "Experimental Results from an Automatic Test Data Generator" *ACM Transactions on Software Engineering and Methods*. Vol. 2 No. 2, April 1993, pp. 109-127
96. R. A. DeMillo, M. Furst, and R. J. Lipton, "Competitive Strategies for k Servers"
97. H. Agrawal, R. A. DeMillo and E. H. Spafford, "Debugging with Dynamic Slicing and Backtracking," *Software Practice & Experience*, June 1993, Vol. 23 No. 6, pp. 589-616
98. R. A. DeMillo, "A Defense of Incremental Research," *International Perspectives on Software Engineering*, June, 1993, Vol. 1, No. 2, pp. 33-36
99. R. A. DeMillo, R. J. Lipton, and A. J. Perlis, "Social Processes and Proofs of Theorems and Programs," *Program Verification*, edited by Timothy R. Colburn, James H. Fetzer, and Terry L. Rankin and published by Kluwer Academic Publishers (1993). *Reprinted. See main entry number [39]*
100. R. A. DeMillo, T-C Li and A. P. Mathur, "A Two Dimensional Scheme to Evaluate the Adequacy of Fault Tolerance Testing," In Third IEEE International Workshop on Integrating Error Models with Fault Injection, pp. 54-56, Annapolis, MD, April, 1994
101. R. A. DeMillo, A. P. Mathur, and E. W. Wong, "Some Critical Remarks on a Hierarchy of Fault Detecting Abilities for Program Testing," *IEEE Transactions on Software Engineering*, 1995
102. R. A. DeMillo, "A Simple Architectural Rule for Conservatively Allocating Software Reliability Requirements,"
103. R. A. DeMillo, "Testability in Software Architectures: Some Definitional Suggestions"
104. R. A. DeMillo and M. Young, "Non-Functional Aspects of Software Architecture Design", *Proceedings Workshop on Software Architectures, 17th International Conference on Software Engineering*, Seattle, Washington, April 1995, pp. 72-79
105. R. A. DeMillo, "Scalability in Software Architectures"
106. R. A. DeMillo and M. Young, "Quantitative Aspects of Software Architecture" *Proceedings of the 15th Annual Software Technology Conference*, Salt Lake City, Utah, April, 1995
107. R. A. DeMillo and D. I. Hmeljak, "C_pk Calibration of the Capability Maturity Model"
108. R. A. DeMillo and R. J. Lipton, "A Gang of Ten Problems in Formal Methods" (unpublished manuscript), 1994 *An earlier version of this paper was presented by the first author at the 1990 ACM Symposium on Test, Analysis and Verification, Victoria, BC*
109. A. Apostolico, G-F. Bilardi, F. Bombi and R. A. DeMillo, "An International Masters Program in Software Engineering: Experience and Prospects" *Proceedings 11th Data Engineering Conference*, Taipei, Taiwan, March 1995

110. R. A. DeMillo, T-C Li, A. P. Mathur, "Using a Hierarchical Failure Mode Set to Assess the Adequacy of Test for Fault-Tolerance," Fourth IEEE International Workshop on Evaluation Techniques for Dependable Systems, 1995
111. R. A. DeMillo, H. Pan, and E. H. Spafford, "Critical Slicing" Proceedings 1996 ACM International Symposium on Software Test and Analysis, San Diego, California, pp. 121-134, January 1996
112. R. A. DeMillo, "Mission-Critical Applications, Commercial Value and Software Quality", ACM Symposium on Strategic Research Directions (June 1996) Boston, Massachusetts.
113. D. Boneh, R. DeMillo and R. J. Lipton, "Encrypted Quantum Measurement" (unpublished manuscript, 1996)
114. L. Osterweil, L. Clarke, R. A. DeMillo, S. F. Feldman, W. McKeeman, E. Miller and J. Salasin, "Strategic Directions in Computing: Software Quality", Symposium on Strategic Research Directions (June 1996) Boston, Massachusetts.
115. R. DeMillo and R. J. Lipton, "Critique of Formal Verification: Alan Perlis and the Seeds of Method and Doubt", in *In the Beginning: Personal Recollections of Software Pioneers* (R. L. Glass, editor) IEEE Computer Society Press (to appear)
116. D. Boneh, R. DeMillo and R. J. Lipton, "On the Importance of Checking Computations" *Eurocrypt 97*, Springer-Verlag, Heidelberg, May 1997
117. R. DeMillo, H. Pan and E. Spafford, "Failure and Fault Analysis for Software Debugging," *Proceedings IEEE COMPSAC*, 1997.
118. R. DeMillo, "The Internet as a Telephone Network", *Educom Review*, Jan/Feb 1998, pp. 12-16.
119. R. A. DeMillo, R. J. Lipton, and A. J. Perlis, "Social Processes and Proofs of Theorems and Programs," *New Directions in the Philosophy of Mathematics* edited by Thomas Tomaszko (Revised and Expanded Edition, 1998), Princeton University Press, pp. 267-286 *Reprinted. See main entry number [40]*
120. D. Boneh, R. A. DeMillo and R. J. Lipton, "On the Importance of Eliminating Errors in Cryptographic Computations," *Journal of Cryptography* 14 (2001) 2, 101-119. See main entry [115]. This paper has been cited many times. It resulted in a revision to the Open SSL Toolkit (rev 0.9.7) requiring a check of the RSA-CRT result.
121. R. A. DeMillo and R. J. Lipton, "Social Processes and Proofs: A Quarter-Century Perspective," Presented to the Royal Society of London, October, 2004.
122. R. C. Basole and R. A. DeMillo, "Information Technology" in *Enterprise Transformation* (edited by W. C. Rouse) Wiley, 2006
123. Richard A. DeMillo, "Keeping Technology Promises," *Communications of the ACM*, November 2012 (Volume 55, No. 11): 37-40.
124. P. M. A. Baker, K. R. Bujak, and R. A. DeMillo, "The Evolving University: Disruptive Change and Institutional Innovation," *Procedia Computer Science*, 14, pp. 330-335.
125. Richard A. DeMillo, "Unbundling Higher Education," in *MOOCs and Open Education Around the World* (edited by Curtis J. Bonk, Mimi Miyoung Lee, Thomas C. Reeves, and Thomas Reynolds) Routledge, 2015.
126. Rafael L. Bras and Richard A. DeMillo, "Leadership Challenges in Higher Education's Digital Future," in *Challenges in Higher Education Leadership*, (edited by James Soto Anthony, Ana Marie Cauce, and Donna Shalala), Routledge, 2017.

E
X
H
I
B
I
T
D

**IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

<p>DONNA CURLING, et al.</p> <p>Plaintiff,</p> <p>vs.</p> <p>BRIAN P. KEMP, et al.</p> <p>Defendant.</p>	<p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p>	<p>CIVIL ACTION FILE NO.: 1:17-cv-2989-AT</p>
---	---	--

DECLARATION OF VIRGINIA MARTIN

VIRGINIA MARTIN hereby declares as follows:

1. I am the Democratic Election Commissioner in Columbia County, New York. I submit this affidavit in support of petitions to use optical scanners with paper ballots to conduct the General Election in the State of Georgia on November 6, 2018.

2. I have been employed as election commissioner since 2008. The role of commissioner in Columbia County is a full-time salaried role overseeing three full-time Democratic staff and 150 or more Democratic seasonal and election-day workers.

3. I hold a BA in English and Communication from Skidmore College and an MS and a PhD in Communication and Rhetoric from Rensselaer Polytechnic Institute. I serve on the advisory board of the National Election Defense Coalition. In the past I have served as a

pollworker in Columbia County, New York. In addition to all the administrative duties of commissioner, I also conduct all training for the pollworkers who handle pollbooks and ballots and, with assistance by my Republican counterpart Jason Nastke, have designed or fine-tuned all of the systems used in our elections.

4. Because of my extensive experience in running secure elections using optical scanners and hand counting a high percentage of the paper ballots therefrom, I have frequently been called to confer with and advise election-integrity experts, attorneys in election cases, other election officials, and other advocates about the security and feasibility of such processes.

5. Columbia County currently has approximately 43,000 active voters in 50 precincts.

6. Since 2010, the Columbia County Board of Elections, comprising Commissioner Nastke and myself, has run 28 elections on Dominion ImageCast optical scan voting machines, followed by a hand count of the voter-marked ballots which I oversee with Commissioner Nastke.

7. New York State was the last state to comply with the Help America Vote Act. This was, as I recall, due to its refusal to adopt any of the then-available systems, which did not meet its standards for accuracy and security, systems which included DREs such as those currently employed by the State of Georgia. To comply with HAVA, New York State demanded modifications of then-available optical-scan systems and successfully secured modifications that it deemed satisfactory from vendors Sequoia Voting Systems, which preceded Dominion, and from ES&S. The system

that New York State demanded was an optical-scan system utilizing voter-marked paper ballots and a post-election hand-count audit. It rejected DRE systems altogether as insecure and unauditible.

8. I have a great deal of experience over dozens of elections overseeing the optical-scan voting, the secure chain of custody, the reconciliation, and the hand-counting of paper ballots. In most elections, multiple races have been hand-counted on each ballot, and in every election, the hand counts were completed efficiently and in a reasonable time frame.

9. I have read in the Coalition Plaintiffs' Motion for Preliminary Injunction Brief the declarations by Matt Bernhard and Logan Lamb, and they are consistent with the academic research on electronic systems that I have consulted during my tenure as commissioner. I have relied on that body of research in establishing the secure and accurate election protocols in use in Columbia County. My reasoning for supporting the use of paper poll books and optically scanned voter-marked paper ballots followed by a robust hand-count audit open to voters, candidates, parties, the public and of course administrators, in Georgia's upcoming election, follows.

10. The vulnerabilities of electronic processes, and particularly those used in elections, are widely known and have been documented for decades by computer scientists in studies that Commissioner Nastke and I have relied on.

11. Therefore, wholly electronic processes are inappropriate for employment in the counting of the votes that every citizen is entitled to cast and to have counted accurately.

12. The electronic processes employed in Georgia's Diebold DRE system electronic poll books are subject to the same vulnerabilities and thus are similarly inappropriate in elections, as revealed in the declarations of Dana Bowers and Jasmine Clark. In my opinion, malfunctioning of electronic processes may be responsible for the difficulties encountered by Robert Kadel, Carri Gibbs Luce, and Laurie Adelholt Mitchell.

13. Optical scanners and voter-marked paper ballots can easily provide for a near-total guarantee that tabulation processes can and will successfully count votes as voters cast them. This can be accomplished by properly securing the paper ballots and by conducting a robust and scientifically sanctioned risk-limiting audit that is open to candidates, parties, voters, and election officials.

14. Securing paper ballots at the poll site and during transport to their ultimate destination for central count is an existing part of the Georgia elections process, given that pollworkers currently secure provisional hand-marked paper ballots marked in the polling place. Securing more ballots will be a very simple process, easily implemented with current written procedures.

15. Voting by voter-marked paper ballot, even when paired with tabulating by optical scanners, provides a means by which vote-counting can be insulated from the vulnerabilities associated with electronic processes. Accusations from Defendants that a paper-ballot process is "Luddite" displays a shocking ignorance of the almost universal findings of computer scientists in the field of election security, virtually all of whom have

concluded that voter-marked paper ballots provide the only secure way to conduct an accurate secret-ballot election.

16. Voter registration processes that are conducted centrally are subject to fewer opportunities for inadvertent or malicious errors to be introduced into voter rolls. Disseminating those processes to poll sites on electronic poll books introduces many more opportunities for problems, as evidenced in the declarations cited above. In my experience using paper poll books (rather than electronic pollbooks), I have never seen voter data concerning party enrollment, precinct, or poll site being inexplicably changed or changed without authorization.

17. It is clear to me that elections in Georgia would gain vast benefit in accuracy, fairness, and voter confidence by reverting to paper poll books, which, in recording their data in hard copy, provide a durable record that cannot with the flip of an electron be changed without explanation and without public notice.

18. Defendants say it is not feasible to transition from a system that employs both DRE and optical-scan voting to a purely optical-scan voting system in time for the November 2018 election. As commissioner I have experience with a major voting-system transition, and it is my opinion that the transition that petitioners propose can be effected smoothly, securely, and effectively for the November election.

19. In September 2010, Commissioner Nastke and I ran the first electronically counted election in Columbia County when New York State mandated a transition from mechanical lever voting machines to a system employing electronically tabulating optical scanners and voter-marked paper

ballots subject to a mandatory hand-count audit. Commissioners in 48 other counties in the state had made a similar transition during a 2009 pilot of the new voting systems, and the remaining 14 made the transition with Columbia County in 2010. I conferred with other such commissioners and exchanged information on processes and administrative changes necessary for this significant transition of voting procedures.

20. During these two years, counties trained inspectors who successfully operated electronic machines and who successfully provided voters with the correct paper ballot for their election. Counties placed paper and ballot-printing orders that were successfully made and filled without difficulty.

21. This and the following November election were the first in which all voters in all counties in the state voted on a system that electronically tabulated votes from hand-marked paper ballots.

22. At the polls, voters were instructed on how to properly mark a ballot, they signed the paper poll book, they were given a paper ballot and a privacy sleeve to shield the voted ballot from prying eyes, and they carried their ballot to a table where they marked their ballot behind the shield of a privacy booth. In the booth, posted instructions could be consulted once again. Voters walked their voted ballot to the optical scanner, where a poll worker provided minimal instruction on how to insert the ballot into the scanner and how to watch the small LCD monitor to determine if their ballot had been successfully scanned.

23. A small minority of voters had any question about how to vote a paper ballot, as it is a simple and routine process. In conducting the post

election hand counts of hundreds of thousands of ballots over the years, my experience is that it is exceptionally rare to encounter a voter's ballot markings that cannot be reasonably interpreted as to the voter's intent. Voters simply ask for a new ballot when they make errors in the marking of their ballot. There is no logical reason to assume that voter confusion will ensue or that hand-marking ballots will cause numerous indeterminable votes.

24. This and the following November election were the first in which poll inspectors were required to understand and manage the proper handling of a wide variety of many new processes, documents, and reports. Most of those processes, documents, and reports had been developed at the state level and introduced to the counties, which then implemented them, as did Commissioner Nastke and I.

25. The transition represented a sea change in how elections are run, changing from a voting mechanism that was solid, immobile, self-contained, impenetrable, and completely mechanical, to a system based on electronic tabulating processes reliant on programming, on voter-marked paper ballots for every single voter, and on far more complicated security protocols. It was a system that featured dozens more moving parts than a lever-based election.

26. While the transition was challenging, it was successfully made. No county failed to procure sufficient ballots, to deploy enough machines, to train enough inspectors, or to have its voters successfully vote. No county failed to conduct the required post-election 3% hand-count audit.

27. In fact, Columbia County successfully conducted a 100% post-election hand-count audit, much more than was required. While it was challenging, it was not impossible and it was successfully completed.

28. What's more, Columbia County developed a simple but airtight chain-of-custody procedure, for ballots and all other election materials, that is initiated immediately upon the close of polls. At close of polls, materials are bipartisanly transported to the Board of Elections to be bipartisanly secured until hand counted in the days following. It has proved to be completely effective and efficient, engenders the confidence of voters, and is the process still in use.

29. In my estimation, Columbia County's and more generally the State of New York's transition from mechanical to electronic voting represents a far greater change, incorporating the introduction of inestimably more complicated processes, than would Coalition Plaintiffs' proposed transition from one electronic voting process to a paper ballot/optical scanning process. The proposed transition is simple in comparison because an existing electronic voting process utilizing DREs and some number of optical scanners tabulating votes on voter-marked paper ballots would shift to a system exclusively of optical scanners tabulating votes on voter-marked paper ballots. Simply put, the proposal is the logical and essential move from one almost completely insecure and unauditable electronic voting process to a secure and auditable one. Even if some administrative inconvenience is incurred in making the near-term transition, it is an essential price to pay to secure the mid-term election.

30. In my estimation, should New York State decide to change to another electronically based election system, that change could be accomplished with far less upset and upheaval than was the change from mechanical to electronic in 2010.

31. In my estimation, and given that the State of Georgia already employs an electronic DRE system, and already employs paper ballots and optical scanners for provisional and mail ballots, and given that many individuals who are voters have encountered optically scanned forms at some point in their lives, the transition from using the electronic DRE machine to an electronic optical scanner should not present an infeasible challenge for election administrators, poll workers, or voters.

32. To lessen the burden of change in the first rollout in November 2018, counties might be provided the option to conduct all scanning centrally, collecting voters' ballots at the poll sites in secure ballot boxes similar to those currently used for provisional ballots. Nevertheless, the operation of an optical scanner is not in my experience a particularly difficult process for a pollworker to master, particularly since Georgia has used the AccuVote optical scanners for over 10 years and many elections.

33. In my estimation, the optical scan system in use in New York State is fairly to very easy for administrators and poll workers to use. It is extremely easy for voters to use. As with the AccuVote system, a paper ballot that has been marked by a voter is fed into the scanner, which then stores it securely. AccuVote scanners are used successfully by temporary Election Day pollworkers in thousands of polling places across the country, and those polling places would generally have no special technically trained

workers. Even if rare mechanical scanner problems are unexpectedly encountered, paper ballots can always be secured and counted later—which is not the case with malfunctioning DRE units.

34. It is my experience as an election commissioner that election boards procure their ballot paper or their printed ballots from vendors far and wide, vendors not limited to the state of residence, that more than one paper stock will perform well in a particular scanner, and that vendors are able and willing to produce ballots that conform to a scanner's specifications.

35. In fact, ES&S, whose DREs the State of Georgia currently uses and with whom its election boards have a working relationship, prints ballots or contracts out ballot printing and would be one logical source for ballots.

36. Another source for ballots would be the counties' current printers for mail and provisional ballots, who simply would need to increase their print runs for every ballot style. All ballot styles are required to be printed under the current election scheme. If they currently print a number of mail ballots equal to 15% of the voter rolls, they would simply need to increase that number by a factor of five or six. In small and modest-sized counties, which the vast majority of the state's counties are, the increase could be easily and probably gladly accommodated. In the larger counties, the increased print runs would represent more of a challenge to printers, but perhaps a sufficient quantity could be made available for the first part of the early-voting period and then the balance provided later.

37. In terms of cost per ballot, in Columbia County, our board prints ballots and provides optical-scanner voting machines for the school

districts in our county. We charge them for our out-of-pocket costs, which for ballot printing include the cost of paper stock and the ballot images made on the board's printer. We also charge a nominal fee for administrative work, some unspecified portion of which would include ballot-related services. Our charge to schools in 2018 was \$1,000 administrative per machine and \$.131 per ballot. If \$250 is attributable to ballot preparation, for a school that purchased a very small but typical run of 2,000 ballots, the actual cost per ballot was \$0.256, considerably less than the \$0.35 per ballot quoted by Defendants. At that rate, for 5,000 ballots, still a small run, the price, assuming administrative costs increased to \$500, would calculate to \$0.152. The economies of scale involved in printing tens of thousands of ballots that simply require shrink wrapping for security purposes may result in prices well below the \$0.35 quoted by State Defendants [Doc.265-6 Bailey Declaration p 3. ¶ 8], even allowing for a reasonable markup.

38. In preparation for this declaration, I interviewed Dave Haines, one of the owners of K&H Integrated Print Solutions, one of the largest ballot printers in the country. He told me that standard ballot printing cost for AccuVote ballots is \$0.26 per ballot, and provided me with customer invoices which are public records for verification of that printing cost for polling place ballots. The standard pricing is consistent with my expectation for market prices of commercial ballot printing.

39. Mr. Haines recommended that Georgia counties can most likely feasibly increase their print runs with their traditional ballot printers who should be able to accommodate them, but his company is prepared to supply ballots to Georgia counties at \$0.26 per ballot on reasonable notice if supply becomes an issue.

40. In preparation for this declaration, one of the election officials I conferred with was Angie Leath, Elections Director in El Paso County, Colorado, a county with approximately 466,000 registered voters, as well as other Colorado election officials. El Paso County conducts elections with hand-marked paper ballots and counts them centrally in the Election Office.

41. I discussed El Paso County's long-time use of the AccuVote Optical Scan system with Ms. Leath. El Paso County upgraded their voting system in 2017 and no longer uses the Diebold AccuVote scanners. Ms. Leath informs me that hourly throughput was 600-800 without problem. Throughput was dependent on the length of the ballot and the number of races on the ballot, with the machine able to throughput the higher number of ballots when the ballot was shorter and had fewer races. The capacity of the 128k memory card was as many as 54 ballot styles, the county's maximum, for a relatively simple election with few races.

42. This throughput rate and capacity is significantly in excess of the estimates in State Defendant's Declaration by Chris Harvey [Doc 265-2, ¶21]. Ms. Leath's estimates of problem-free high-volume throughput were consistent with other election officials I conferred with who have personally used AccuVote scanners in relatively high-volume central-count operations without problems.

43. No official I talked with reported instances of AccuVote scanners "breaking" or malfunctioning because of volume, despite Merritt Beaver's concerns expressed in Document 265-1 ¶ 9.

44. Ms. Leath informed me that El Paso County currently has 250-300 AccuVote Optical Scanners in storage, along with a similar number of

black-box units on which each sits and into which ballots can securely drop after scanning, both of which can be made available for sale. It is my understanding that the market value of used AccuVote scanners is very weak and prices are low, as evidenced by the fact that Adams County, Colorado gave Georgia 154 AccuVote scanners in 2016 for the cost of transportation. (<https://www.ledger-enquirer.com/news/politics-government/election/article96275322.html>)

45. Concerns relating to AccuVote scanner availability expressed by Georgia's officials in their declarations suggest that they misunderstand the current state of the market for this older equipment.

46. In our conversation concerning the availability of ballot printing for AccuVote scanning, Ms. Leath informed me that the paper used in the AccuVote Optical Scanner is a common paper, and that El Paso County used Springhill 80 pound stock.

47. My conversations with election officials who have recently used and studied AccuVote scanners in high-volume operations caused me to conclude that scanning equipment and ballot-printing capacity should be reasonably available for the November 2018 election.

48. I have reviewed public records information obtained from Henry County, Georgia and Morgan County Georgia, regarding operating experience with and availability of optical scanners, and ballot printing orders, all of which have informed my opinion that adequate AccuVote ballot scanning capacity is readily available and that Georgia's experience, like other states', is that the system is reliable and generally mechanically trouble-free.

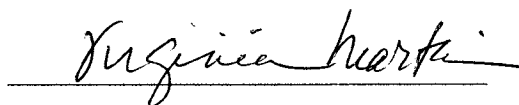
49. It is my experience as an election commissioner that voters gain great confidence and reassurance from casting their votes on a paper ballot that they know survives election day and can be examined to verify their votes. It is my experience that voters are horrified that some jurisdictions, thankfully none in New York State, conduct elections without verifiable paper ballots. It is my experience that voters in my county are exceedingly confident that the vote counts that Commissioner Nastke and I certify and which they are welcome to attend and closely observe are absolutely correct.

50. It is my experience as an election commissioner that voters are reassured by the presence of non-electronic pen and paper processes at the polls, as present in our paper poll books and our paper ballots. Many voters are skeptical of the mutable and hackable nature of electronic processes as they have been introduced into elections, especially in light of the last two years news of foreign nation-state election hacking attempts.

51. I as commissioner would not certify an election if I could not personally know, via non-electronic means, either by my own visual examination or that of other trusted individuals, that the vote totals as calculated are accurate. I so testified to the New York State Assembly Election Law Committee in 2010 before the transition to electronic voting machines was made. Since that transition, both Commissioner Nastke and I have personally or through trusted individuals verified the accuracy of vote totals in every election. We have done so efficiently, quickly, and without incurring high costs.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, August 20, 2018.

A handwritten signature in cursive script, reading "Virginia Martin", written in black ink over a horizontal line.

Virginia Martin

E
X
H
I
B
I
T
E

**IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

DONNA CURLING, et al.

Plaintiff,

vs.

BRIAN P. KEMP, et al.

Defendant.

**CIVIL ACTION FILE NO.:
1:17-cv-2989-AT**

DECLARATION OF AMBER F. McREYNOLDS

AMBER F. McREYNOLDS hereby declares as follows:

1. I am currently the Executive Director for the Vote At Home Institute and Coalition focused on improving the voting experience for voters across the country and implementing convenient voting options to include effective ballot delivery systems (commonly known as ballots by mail) along with in person voting options to ensure voters have convenient options.
2. Until August 15, 2018, I was the Elections Director for the City and County of Denver. I administered elections in Denver for 13 years and have worked in public policy and administration for over 16 years. I served as the Director of Elections for the past 7 years, Deputy Director of

Elections from 2008 to 2011, and Operations Manager/Coordinator from 2005-2008.

3. Denver has approximately 500,000 registered voters and conducts 2-4 elections each year. The elections include municipal general and municipal run-off, school board, special district, primary, general, presidential.

4. My educational background is as follows:

a. Education:

- Masters of Science – Comparative Politics, London School of Economics & Political Science, 2002
- Bachelor of Arts – Political Science and Speech Communications, University of Illinois, 2001

b. Professional Certifications:

- Certified Elections/Registration Administrator (CERA), Election Center (2010 – Present)
- Certified Colorado Election Official (2007 – Present)
- GOALS Program, City and County of Denver

c. Professional Memberships and Affiliations:

- Advisory Committee, MIT Election Data and Science Lab
- The Election Center (National Association of Election Officials)
- Circle of Advisors, Democracy Fund, Election Validation Project
- International Association of Government Officials (iGO)
- Colorado County Clerks Association
- Denver Metro Chamber of Commerce
- Leadership Denver 2016-2017, Denver Leadership Foundation
- Women's Foundation of Colorado

- Metro Denver Chamber of Commerce
- Women's Chamber of Commerce, Denver, Colorado
- Project Management International
- Alumni and Friends of the London School of Economics USA
- University of Illinois Alumni Association
- Mentor – Humphrey School of Public Affairs – University of Minnesota

5. I was qualified as an expert witness in the field of elections, in the Civil Action No. 17-02016 (RC), U.S. District Court for the District of Columbia (2017) and Gessler v. Johnson, 2011CV6588, Denver District Court (2013).
6. In my role as the Director of Elections in Denver, I focused on continual process improvement which includes implementing innovative solutions to improve the voter's experience. During my tenure, the Denver Elections Division earned national awards from the Election Center and the National Association of Counties for Ballot TRACE (a first-in-the-nation ballot tracking, reporting, and communication engine), iAPP (iPad Accessibility Pilot Project), and eSign (a first-in-the-nation Digital Petition and Voter Registration Drive Application). Denver has also been recognized by the International Centre for Parliamentary Studies and received International Electoral Awards for Ballot TRACE and eSign. In addition, the Denver Elections Division has released other innovative solutions including the

Denver Votes mobile application, enhanced contextual and behavioral marketing strategies to encourage civic engagement, interactive customer service platforms, and implemented a new voting system in 2015.

7. I am committed to conducting and promoting fair, accessible, secure, transparent, and efficient elections. I currently serve on the Council of State Government's Overseas Voting Initiative's Technology Committee, Advisory Committee of the MIT Election and Data Science Lab, Circle of Advisors for the Democracy Fund's Election Validation Project, and various statewide and national committees and working groups.
8. I have served as an election expert witness, assisted with legislative and policy development, and have been invited to participate with various national and state professional organizations to identify and implement best practices in election administration. Denver has become a national leader in election management and innovation and officials from around the country and the world visit regularly to learn best practices.
9. Denver has conducted post-election audits for the entire time that I was Director and prior to that. The purpose of post-election audits is to verify that the outcomes of the electronically counted ballots are correct to a predetermined statistical probability. Because all computerized election equipment is subject to risk of cyberattacks, it is necessary to test that the

outcomes reflect the voters intent as expressed on their individual voter verified ballots.

10. Denver recently converted from a random post-election audit to a risk-limiting audit procedure in 2017 and will continue Risk-Limiting Audits indefinitely. Risk Limiting Audits are a more sophisticated method of auditing and reduces the sample size needed to attain assurance of the correct outcome.
11. Beginning in 2008, Denver began converting from a predominantly DRE based voting model at polling locations and early voting locations to a predominantly paper based system (with a limited DRE option for accessibility requirements).
 - a. I served as the Deputy Director of Elections during this conversion.
 - b. During 2008, Permanent Mail-In Voting went into effect and we saw an increase in requests for mail-in ballots. 62% of the Votes cast in the 2008 Presidential Election were mail-in ballots. 19% were cast at polling places. 18% were cast during in-person early voting. The total turnout during the 2008 Presidential Election was 89% active voters, 67% overall including inactive voters.
 - c. Denver utilizes a central count environment and has done so before and after the 2013 voting model conversion. This means that every single

vote is tabulated and tallied in the election headquarters, not at each individual voting location.

12. The paper ballots are secured from the point they are cast in vote centers, placed in drop boxes, or delivered to post office throughout the process of counting and 25 month ballot retention period.. Paper ballots require chain of custody logs and security, easily understood by pollworkers. Bi-partisan ballot security teams transport the paper ballots from the Vote Centers (Polling Places prior to 2013) to the central counting facility.

INITIATING A VERIFIABLE ELECTION—CORRECTING THE ELECTRONIC POLLBOOK RECORDS

13. An indispensable fundamental element of conducting a verifiable election is assuring that voter registration files are accurate and that the pollbooks reflect that accuracy to prevent voter disenfranchisement and confusion at the polls.
14. The electronic pollbooks (Diebold ExpressPoll units) are a key component of Georgia's certified DRE-based voting system. The electronic pollbooks are integral components in the Diebold voting system as used in Georgia as the electronic pollbooks generate and code the voter access card with the electronic ballot style for activating and presenting the correct ballot on the DRE.

15. I have read in the Coalition's Motion for Preliminary Injunction Brief the examples of discrepancies and voter problems that appear to be caused by corrupted files in the electronic pollbook and/or the master voter registration files. Such discrepancies and errors must be urgently corrected in all counties in order to conduct a fair and accurate election in November.
16. Even if the voter registration files are accurate and updated, if ExpressPollbook data discrepancies are present, such as those described in the Exhibits to the Coalition Plaintiffs' Motion as the pollbooks qualify voters at the polling place, a fair election will be difficult to conduct. Voters will be disenfranchised when they must vote provisional ballots in the "wrong" precinct which may not offer the voter all the candidates and contest for which they are eligible to vote. In fact, it will be almost impossible in real time to determine the correct precinct and ballot style for the voter, if such discrepancies are not corrected at a system level.
17. The ExpressPollbook data can potentially be corrupted by multiple means, including being connected to and interacting with other corrupted electronic components of the DRE voting system.
18. It cannot be overemphasized that both accurate pollbooks and voter-verified paper ballots (or a paper audit trail) are required for the conduct of a fair and accurate election.

19. It is imperative that correction of DRE system electronic pollbook and voter registration records and the reconciliation of discrepancies between the two records be undertaken immediately as a serious effort. Researching, confirming accurate information, and correcting errors will likely take weeks of work and must begin immediately, regardless of what voting system is used in November's election.
20. Given the significant problems that appear to be of unknown origin in the electronic pollbooks and the general need for verification of auditable records, I recommend initiating an audit (perhaps by another state agency with auditing capabilities or an outside entity with expertise in database auditing) to review the pollbook set-up and review discrepancies documented previously. I further recommend that a back-up (paper or other) be allocated to each polling location to ensure efficient and accurate voter processing.

NECESSITY OF PAPER BALLOTS WITH AUDIT TRAIL

21. In my professional experience, given the technology that is available today, a paper ballot with a voter-verified audit trail is unquestionably essential in election and voting systems. Colorado has primarily voted on paper ballots for a long period of time, with only a short period in the mid-2000's where DRE systems were used in some counties, but

were soon abandoned for reliable and verifiable paper ballot systems.

Denver converted to a primarily paper ballot based system in 2008.

22. After years of developing supporting procedures, regulation and statutory requirements for high volume mail ballot processing, in 2013, the Colorado legislature passed a bill to mandate mail ballots, with exceptions made for in-person vote centers for voters wishing to cast their ballots in person. This system replaced a traditional system of voting paper ballots in the neighborhood precincts counted by precinct optical scanners or central count optical scanners, depending on the county.
23. Under Colorado's current law and with its ballot delivery system, every voter is automatically mailed a paper ballot, and voters also have the option of voting in person at a vote center also on a paper ballot, even if using the accessible ballot marking device. It is essential to use a voting system under which the voter directly records their vote on paper, or on a voter-verifiable paper record.
24. Virtually all Colorado counties count the paper ballots with optical scanners located centrally at each counties' election office, with results tabulated on each counties' election management server from which reports are generated. In the case of a very small number of sparsely

populated counties, hand counts of paper ballots continue to be used successfully.

25. Colorado has long recognized the necessity of a voter-verified paper record of voters' intent as required by HAVA. Without such a paper record created or verified by the voter, the results cannot be audited, recounted or otherwise verified. Post-election audits of computer tabulations and reports have been required by Colorado law for many years. Beginning in 2017, sophisticated Risk Limiting Audits were mandated to gain statistically valid assurance that reported election outcomes are correct.
26. Post-election auditing is essential because it is well understood by election professionals that all computerized election operations are vulnerable to error or malicious interference and cannot be accepted as accurate without appropriate post-election testing. Post-election auditing, conducted in public with oversight and involvement by bipartisan officials, must be successfully completed before Colorado county citizen-run election boards certify the election results.
27. Paper ballots counted by optical scanners alone are not enough to ensure an accurate count. In Georgia's case, the Accu-Vote optical scanners and GEMS server's output must be audited to be confident

that no material errors, programming mistakes, or hacking has impacted the results.

28. It is essential that Georgia conduct post-election audits for paper ballots counted on optical scanners and summarized on the election management system server (GEMS server.) This fundamental requirement is true for all electronically counted ballots, but the need is even more undispensible because Georgia's voting system components were exposed to the risk of anonymous malicious users while programs were on the server at KSU.
29. Numerous expert resources are available at little nor no cost to advise Georgia jurisdictions on implementing various types of post-election audits of paper ballot elections. In my experience, the election community shares best practices and aids our fellow colleagues in urgent circumstances.
30. There is virtually universal agreement by election officials and voting system experts that paperless DREs, such as Georgia uses, cannot be meaningfully audited or recounted, and that verifiable elections require a voter-verified paper audit trail.
31. Georgia was granted \$10.8 million in HAVA funding very recently. Post election audit programs are a qualified use of HAVA funds, and

Georgia can use such funds to implement a program for November's election.

**PAPER BALLOT PROCESSING
INCLUDING SIGNATURE VERIFICATION**

32. I concur with Coalition Plaintiffs' recommendation that paper ballots be issued in the polling place with currently owned Accu-vote optical scanners used for ballot counting and GEMS servers used for consolidated tabulation and report generation. I describe below Colorado's paper ballot processing and ballot security system to explain the feasibility of Georgia's use of paper ballots and the necessity of, but easily implemented security controls over paper ballots.
33. A key difference between Denver's current system of voting and the Coalition Plaintiffs' proposed method in Georgia is the very high component (95%+) of mail ballot voting in Denver. Extensive mail ballot voting is not currently appropriate for Georgia because of Georgia's limited procedural requirements and controls for protecting mail ballot voters. However, paper ballot security and processing requirements between the two methods are similar and based on the same principals. The remaining percentage of votes cast in Denver are on paper and the counting procedures are consistent for each and every ballot cast in Colorado. This

is different in Georgia because ballots are counted and tabulated differently with the variance in the types ballots cast.

34. After ballots are returned to the Denver election office's via mail, dedicated secure drop boxes positioned throughout the county, or in-person vote center secured ballot boxes, processes developed over several years are used to verify signatures of voters to confirm their eligibility to vote.
35. The signature verification process for large numbers of mail ballot voters requires electronic files of multiple exemplar signatures for voters, bi-partisan teams of trained signature verification officials, escalation and adjudication rules for discrepant signatures, adequate notification of voters to permit cures of non-matching signatures, 8 days of time after election day to cure signatures, and detailed regulations for the fair adjudication of signature verification.
36. Signature verification of mail ballot envelopes can be a subjective process that requires well-considered rules, bi-partisan decision making, trained workers, bi-partisan oversight and opportunities to challenge officials' questionable acceptance or rejection decisions, and multiple levels of decision review before a ballot is rejected to be set aside for the cure process. Most large Colorado counties use automated signature verification computer equipment to assist in the initial reviews of signatures with

statistical audits to verify the accuracy of automated signature verification process.

37. It is my understanding the Georgia election code does not require bi-partisan signature review before signature and ballot rejection, nor bi-partisan oversight or challenge opportunities of the process. It is also my understanding that mail ballot voters do not have an opportunity to cure signatures that appear to have discrepancies before they are disenfranchised by ballot rejection. This makes the widespread use of mail ballots a risky process with a high possibility of eligible voters being disenfranchised if their signatures are judged to not match their voter registration records and/or their mail ballot application. It is my experience that many legitimate voter signatures do not initially match older registration records and can be improperly rejected without a trained bi-partisan review process with appropriate checks and balances and a fair opportunity for the voter to cure the apparent signature discrepancy. Thus, I would recommend modifications to the above processes in preparation for the November Election, especially with the potential for an increase in the use of mail ballot voting.
38. Colorado voters are aware that their signatures are tested against numerous previous signature on official documents such as voter registration records,

previous ballot envelope signatures, driver's license application signatures, and other official records, and know to carefully sign their ballot envelopes. It is my understanding that Georgia does not compare multiple signatures from such records, and Georgia voters may not be educated on the strict match process that allows little room for error, without an opportunity to cure discrepancies.

39. I believe that that risk of voter disenfranchisement exists that makes it unduly risky for Georgia voters to vote by mail ballots without the ability to cure legitimate but signatures judged to be discrepant. It is also concerning that partisan decision making could enter the signature approval process without bi-partisan team oversight or a chance to challenge signature rejection. Colorado law, rules and formal policies protect the voters from this risk of disenfranchisement and from fraud that could be perpetrated by illegal signatures on ballot envelopes.
40. Georgia's mail ballot laws greatly restrict the casting of mail ballots on Election Day by requiring personal hand delivery to the central office, prohibiting polling place drop off. A large percentage of voters prefer to vote on Election Day to wait to consider all late breaking news in campaigns and conduct their last minute study of the races. Georgia's requirement that each mail ballot cast on Election Day be in-person by the

voter himself at the central office, discourages mail ballot voting, particularly given the traffic in Atlanta and other locations. I would suggest modifications to this process to allow voters to drop off their mail ballot at any polling location across Georgia.

41. Georgia ranked 42nd for Mail Ballots Rejected on the recent Election Performance Index <https://elections.mit.edu/#state-GA>. This illustrates why I have concerns about the increase in the use of mail ballots without modifications to the existing process.
42. In the absence of a signature cure process, efficient drop-off procedures and locations, and other procedures, the claim that voters can protect themselves by using a mail ballot as opposed to a potentially unreliable DRE without a paper audit trail is not a legitimate replacement. In my professional opinion, the current mail ballot procedures need to be updated in advance of this November election to ensure voters have fair and accessible options.

**FEASIBILITY OF IMMEDIATE CONVERSION
TO PAPER BALLOTS**

43. In my opinion, with appropriate and efficient planning, best practices, and assistance from experts in the field, Georgia has time to convert to paper ballots in an organized manner because no new technology, systems

conversion, or significant training is needed. This is primarily because it is my understanding that Georgia uses an adequate paper ballot scanning and tabulation system currently, which can be successfully deployed system wide if post-election audits are required, and electronic pollbooks are corrected and backed up with paper pollbooks. Additionally, there are available resources and plans from states with a similar system that can be utilized quickly.

44. I understand that Georgia has certified and uses Diebold Accu-vote TS and TSx paperless DRE units for in person voting, in concert with Accu-Vote Optical Scan for paper mail and provisional ballots, tabulated by the GEMS server.
45. I am familiar with this equipment through its widespread and successful use in Colorado in prior years, although Denver did not use the Diebold brand of optical scanners. Denver used Sequoia 400c high speed optical scanners prior to May 2015 when the new Dominion system that includes high-speed Canon optical scanners was deployed. Some counties in Colorado did use the AccuVote Optical scanners in a central count environment.
46. Although Diebold Accu-vote optical scanners are not the most modern or highest speed ballot scanners, they are in successful widespread use across

the country. I have reviewed Verified Voting's summary of installed election equipment at <https://www.verifiedvoting.org/verifier/> which shows that Diebold AccuVote scanners are used in over 400 counties and 20,750 precincts and central county operations.

47. It is my understanding that Georgia currently has approximately 900 AccuVote optical scanners currently in inventory and available for use.
48. Based on my knowledge of the market for election equipment, and discussions with vendors and other election officials, if additional AccuVote optical scanning units needed, there is significant used inventory available since many states have converted to new systems. In my research, I found that El Paso County in Colorado has 250-300 scanners available. There is also new AccuVote inventory available from vendors.
49. I understand that in 2016, Adams County, CO gave Georgia 154 such scanners. (reference footnote <https://www.ledger-enquirer.com/news/politics-government/election/article96275322.html>). I believe that other scanners may be available from other jurisdictions in Colorado and elsewhere, as well as from vendors. The cost of such optical scanners should be quite affordable.
50. In March 2018 Congress appropriated \$380 million in additional HAVA funding for states including and specifically encouraging purchasing

security improvement election equipment, such as optical scanners for ballot counting. As well, activities that improve security of the computer systems are eligible for the grant money, which should include the updating of the electronic pollbook data and security. Georgia's share of these immediately available funds is \$10.8 million.

[\(https://www.eac.gov/2018-hava-election-security-funds/\)](https://www.eac.gov/2018-hava-election-security-funds/).

51. Diebold Accu-Vote optical scan equipment is expected to scan at approximately 30 ballots per minute. I have conferred with long time users of Accu-Vote scanners in high ballot volume processing and feel confident that Georgia has adequate optical scanning capacity and could readily acquire more capacity at affordable or minimal cost.
52. San Diego County, California, with approximately 1.7 million voters uses Diebold Accu-vote OS machines (of the type Georgia uses) in a central count operation for nearly 1,000,000 ballots, which is indicative of the volumes that these scanners can handle in a complex ballot style environment.
53. In my inquiries for this declaration, I conferred with Stan Martin, Adams County, Colorado Clerk & Recorder. Adams County gave Georgia 154 Accu-Vote scanners in 2016. Adams County has approximately 350,000 registered voters and used these scanners successfully in a central count

installation for several years, without reports of “overheating” or “breaking” as has been stated as a concern by the State Defendants at Merritt Beaver’s Declaration (Doc. 265-1, ¶9)

54. I recommend a central count environment, rather than a precinct scanning operation, although it is my understanding that Georgia law permits either type of scanning with certified voting system scanners. Based on my experience, a central count environment mitigates risk with technology and tabulation in the field. It is likely preferable for workers already familiar with the scanner use operate them when with a near term change is being implemented.
55. With a central count environment, secured ballot boxes can be transported to the counting facility, chain of custody procedures can be implemented to ensure complete accounting, and security procedures can be put in place (bi-partisan teams, field accounting procedures) to ensure an effective and secure transport mechanism from the field to the central facility. Such procedures are already in place in handling provisional paper ballots voted in the polling places on Election Day.
56. Election central office workers are already trained on Accu-vote optical scanning machines and have successfully processed mail and provisional ballots on these scanners for over a decade.

57. Converting from a DRE model to a predominantly paper based model is a change but not particularly complicated, especially considering that Georgia already produces and utilizes paper ballots for mail voting and provisional ballot voting. Some Colorado counties, such as Jefferson County (434,000 registered voters) used DREs in conjunction with optical scanners and made a smooth transition to paper based voting continuing to use its optical scanners in its older voting system (as Coalition Plaintiffs suggest here), until a new voting system was selected several years later.

PAPER BALLOT VOTING AND PROCESSING

58. The voter check-in process through the electronic pollbook (with recommended paper backup) would remain the same as it is now in the polling place, with the voter being issued a paper ballot rather than voter DRE machine access card.
59. Hand marked paper ballots will not require voter education. Voters know how to mark paper ballots easily following instructions to mark with the permanent ink markers provided, by coloring in the oval beside the candidate's name or ballot choice. I would recommend that Georgia follow best practices for ballot design utilizing the Center for Civic Design guidelines.

60. These voters would mark the ballot privately, protected by a privacy shield, which can be inexpensively fashioned from stiff card stock, cardboard, or plastic, and then place the ballot in a secured ballot box with chain of custody controls (there are various methods and best practices available to ensure a smooth transition) similar to the chain of custody controls used now on the locked provisional ballot box used in the polling places. Also, counties across the U.S. that have converted from polling place models to vote centers or primarily mail ballots have also made use of privacy booths available. Denver and other Colorado counties gave booths away in the conversion.
61. Handling paper ballots in a secure way with chain of custody documentation is routine across US elections, including at precinct polling places, and vote centers such as those used by Colorado for in person voting.
62. Training pollworkers to issue ballots will be far less complex than training workers to deal with the set up, testing, securing and trouble-shooting and problem resolution that is required for DRE operation in the polling place. After all, Georgia pollworkers currently issue and secure control and account for paper provisional ballots in the polling place on Election Day.

63. DRE delivery, set up, testing, security, close down, memory card collection and returning DREs to the warehouse is an inherently labor intensive expensive process, and requires considerably more manpower, including skilled DRE operation, than does the delivery of a package of shrink-wrapped paper ballots in sealed boxes to the polling place.
64. Counties which use hourly or contract personnel to program, test, deliver, secure or set up the DRE machines, should be expected to experience a cost savings by avoiding such labor intensive work in favor of delivering a secure package of paper ballots and other election supplies.
65. Mid-day transfer of secured ballot boxes (replaced with empty secured ballot boxes) can accelerate scanning on Election Day afternoon or staging for post-poll closing, to accelerate the ballot scanning at the time scanning is authorized before closing of the polls.
66. Ballot inventory controls should be implemented in similar way to the daily recap sheet currently prepared reconciling the number of ballots cast to the number of voters checked in for voting at the polls.
67. If mid-day transfer is not used, the locked ballot box with chain of custody records along with poll administration documents would be returned to the county central count location for processing by optical scanners.

68. Accu-vote optical scanners process ballots at the stated approximate rate of 30 ballots per minute. At the end of the scanning, workers insert an “ender card” to mark the completion of scanning, signaling the machine to begin automated tabulation of the scanned ballots. This is the same procedure used today for counting and processing of mail ballots and provisional ballots.
69. Upon the completion of scanning the memory cards from the scanners are uploaded to the GEMS server where tabulation and report generation is performed on a consolidated election basis. This is the same process used today.

EARLY VOTING CONSIDERATIONS

70. Fulton County Board of Elections states that it will reduce the early voting locations to one location if paper ballots are mandated by this Court. [Doc. 267 p. 38 ¶ 21]
71. The rationale for Fulton’s threat seems to be that early voting locations would be required to issue paper ballots for up to 377 precincts, a process now done automatically, but questionable accuracy, by the DRE voting system and the electronic pollbooks.
72. In my opinion, greatly reducing early voting sites is an unnecessary over-reaction to the need to have paper ballots in early voting locations. There

are two generally accepted solutions that can be used alone or in tandem in large counties with many early voting locations—maintaining an organized inventory of paper ballots, or using “ballot on demand” printers at the early voting locations. Small counties with limited early voting locations and limited numbers of precincts should not have an issue with paper ballot inventory control, nor need “ballot on demand” printers.

73. “Ballot on demand” printers are owned by some Georgia counties now, and routinely used in almost all Colorado counties for producing ballots for all ballot styles on an as needed basis. Ballot on demand printers could be utilized in Georgia in early voting locations, backed up by a safety stock of paper ballots in case of technical difficulties. Paper ballot inventory can be easily restocked from the central elections office or annex offices in other parts of the county if ballot inventory runs low.
74. Although maintaining paper ballot inventory for 377 precincts in Fulton County would be slightly cumbersome and administratively inconvenient, it is not an administrative burden that would justify the shutdown of early voting locations in my opinion. It is merely a matter of carefully securely storing the inventory in an organized fashion, and carefully checking ballot style number before issuing to the voter. In Denver, there were 426 precincts and we successfully conducted early voting for over 50,000

voters at 13 different locations during the 2008 Presidential Election. We utilized secure storage units with individual shelves for each ballot style. The units were securely locked and used to store the precinct inventory for each site securely.

75. Issuing paper ballots in the polling place and in early voting makes it much easier for officials and voters to visually detect an error in ballot issuance and to issue a correct ballot to a voter than if the ballot is not on a paper record that can be viewed by workers and voters. If the ballot is merely an electronic ballot buried in a machine, it is far more likely that ballot issuance errors will go undetected.
76. Paper ballots in the early voting polling places should be rigorously secured nightly with chain of custody documents with a schedule for secured ballot boxes to be frequently delivered to the county election office by bi-partisan teams that have specific security credentials.
77. It is my understanding that in the current early voting process, memory cards are left in the DRE voting machines every night during early voting and not removed from the machines and secured until Election Day. The DRE machines and memory cards cannot be properly secured in early voting locations like libraries, churches and recreation centers, leaving machines and memory cards, and therefore the entire county's system

vulnerable to undetectable malicious attack by implanting malware in just one machine or one memory card. Paper ballots, on the other hand, can be and should be physically secured at all times, with chain of custody logs and surveillance to make any tampering both limited (one ballot box) and detectable.

AVAILABILITY OF PAPER BALLOTS

78. Accu-Vote OS ballots are printed by numerous commercial ballot printers across country, and should be reasonably available, given the widespread use of Accu-vote Optical Scanners. Based on my discussions with large ballot printers for purposes of his declaration, if ballots were ordered by mid-September, ballot printing should cost approximately \$.26 per ballot--- 25% less than the print cost quoted by Richmond County. [Bailey Declaration Doc. 265-6 ¶ 8]
79. Ballot set up and printing is already planned for every ballot style as absentee mail and provisional ballots must be printed even under the current system. Ballot printers have told me that increasing the print run size should not create a significant problem in timely delivery.
80. Paper ballots can be delivered and secured the night before Election Day at polling place. Polling place ballot quantities are not difficult to transport. In Denver, we delivered paper ballot quantities to polling places with secure

packaging and seals. The chain of custody procedures (opening the ballot boxes and showing all polling place workers that the ballot box is empty at the start is key).

VOTER CONSIDERATIONS

81. My opinion based on my experience with Denver's voters and the opinion shared by other election officials with whom I have conferred is that voters have little difficulty in instinctively knowing how to vote a paper ballot, marking the choices by filling in ovals on their ballot. Georgia voters will have no trouble marking their choices on a paper ballot, as they do in community elections in their unions, churches, home owners' associations, etc. Additionally, since 2016 and with the constant news coverage about reliability of voting systems, we are seeing more voters requesting paper ballots or a ballot marking device that produces a paper ballot.
82. Marking a paper ballot will be faster than operating the DRE for many voters, particularly those who are not confident of using computers to vote, or voting on the machines that have calibration issues that cause delays. As I have conferred with other election officials in preparation for this opinion, I confirmed that other officials that have used the same system as Georgia saw a decrease in the time to vote when converting to primarily paper ballots instead of this DRE.

83. Based on my experience with voters and pollworkers, it is my opinion that voting by paper ballot will generate increased voter confidence in the process and the announced election outcome. Knowing that there is an auditable paper trail for use in a recount or challenge is a confidence-building fact for voters.
84. The number of votes on paper ballots that cannot be interpreted for voter intent by a review board is miniscule in my experience. I believe that the percentage of such ballots has historically been below .00025% in Denver. Conversely, the number of touchscreen mistakes cannot be known or measured, but unlike paper ballots, choices cannot be verified by the voter as they can be confident of their votes on paper.

SUMMARY

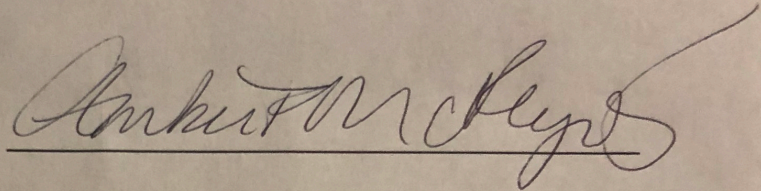
85. Election officials naturally worry about changing processes. Also, election administration is about people and process and especially risk mitigation. Because it is primarily people and process, there is not a perfect system or perfect environment. However, it is critical to mitigate and reduce risk wherever possible and this is where my experience running the election process in various voting models matters. In my opinion, making the change to paper ballots is a low risk change to avoid high risk of potential failure (which may be undetectable) of the electronic DRE voting system.

86. While administrative errors will be made and some machines will have problems in all elections, recovery from errors is almost always possible in paper ballot elections where audit trails exist.
87. Voters generally know how to mark paper ballots, and election workers know how to handle, issue and secure paper ballots in the same way they do now for provisional voters.
88. The Accu-Vote optical scanning system used today in Georgia for paper ballots is widely used across the United States, with a consistent record of mechanical efficiency and durability, although as with any ballot scanning system, post-election audits are necessary. Fears of widespread or chronic scanner breakdowns appear unfounded based on my research.
89. In my opinion, the Defendants and all county election officials, without waiting for this Court's ruling, should immediately undertake a systematic review of the accuracy of the voter registration database and assure that the Diebold electronic pollbooks are operating properly with the identical relevant data in the voter registration base, and correct the discrepancies reported in recent elections and the underlying cause. I would also recommend engaging an outside entity to review the database. This is a best practice in the industry and there are various resources available.

90. In my opinion, the adoption of paper ballots in the polling places can be done in a responsible manner in advance of the November elections, albeit with some administrative inconvenience and change. Voters will be greatly advantaged by conducting an election that is verifiable and complies with law. Risk of voter confusion about the act of voting a paper ballot is non-existent and in fact, voters may start choosing paper ballots given the constant news about electronic (without a paper back-up) systems.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, August 20, 2018.

A handwritten signature in cursive script, reading "Amber F. McReynolds", written in dark ink. The signature is positioned above a horizontal line.

Amber F. McReynolds

E
X
H
I
B
I
T
F

Current Diebold Voting System



DRE MACHINE



ELECTRONIC POLL BOOK



GEMS SERVER



PAPER BALLOT SCANNER

Proposed Diebold Voting System



DRE MACHINE



ELECTRONIC POLL BOOK



GEMS SERVER

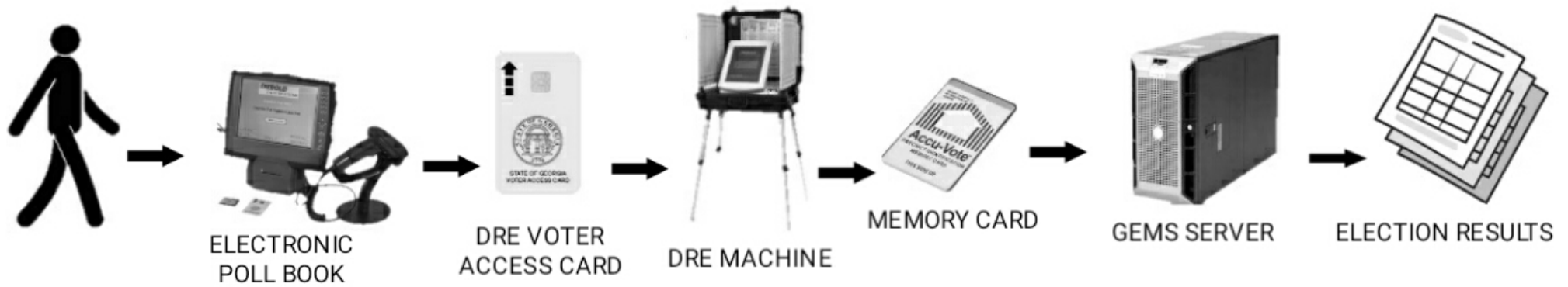


PAPER BALLOT SCANNER

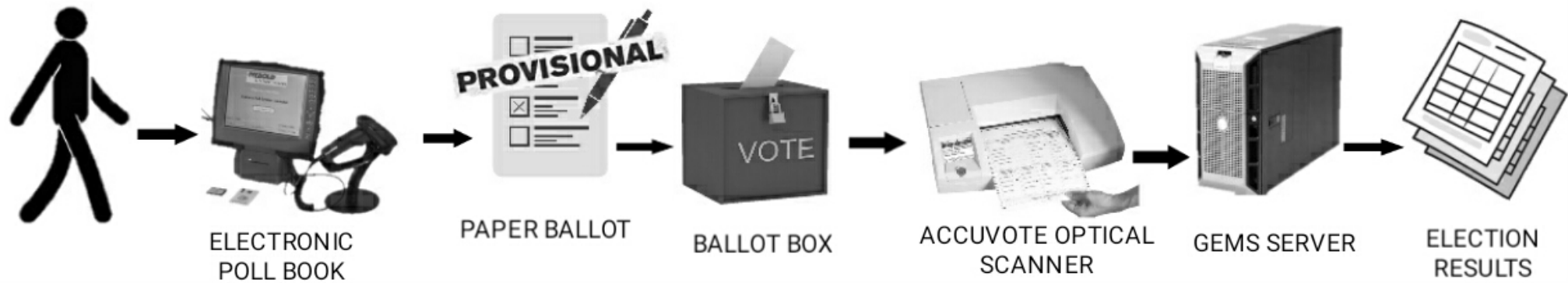
E
X
H
I
B
I
T

G

CURRENT DRE SYSTEM: IN-PERSON VOTING



CURRENT PROVISIONAL VOTING: AT POLLING PLACE



PROPOSED PAPER BALLOT SYSTEM: IN-PERSON VOTING

