2019 WL 3822123
United States District Court, N.D. Georgia, Atlanta Division.

Donna CURLING, et al., Plaintiffs,
v.
Brad RAFFENSPERGER, et al., Defendants.

CIVIL ACTION NO. 1:17-CV-2989-AT
|
Signed 08/15/2019

Synopsis

Background: Voters brought § 1983 action against state election officials in state court alleging that use of electronic voting machines that did not produce paper audit trail diminished and burdened their First and Fourteenth Amendment rights to cast a properly-counted vote. Following removal, voters moved for a preliminary injunction prohibiting defendants from using electronic voting mechanisms and requiring defendants to use hand-marked paper ballots in upcoming elections.

Holdings: The District Court, Amy Totenberg, J., held that:

municipalities that conducted their own elections were not necessary parties;

voters had substantial likelihood of prevailing on merits of their claim;

with respect to future elections after upcoming off-year local and municipal elections, balance of hardships and public interest supported grant of preliminary injunction; but

with respect to upcoming off-year local and municipal elections, balance of hardships and public interest did not support grant of preliminary injunction.

Motions granted in part and denied in part.

Attorneys and Law Firms

Cameron A. Tepfer, Catherine L. Chapple, David D. Cross, Jane P. Bentrott, John P. Carlin, Marcie Brimer, Robert W. Manoso, Morrison & Foerster, LLP-DC, David R. Brody, Pro Hac Vice, Jacob Paul Conarck, Ezra David Rosenberg, John Michael Powers, Lawyers' Committee for Civil Rights Under Law, Washington, DC, Robert Alexander McGuire, III, Robert McGuire Law Firm, Seattle, WA, Adam Martin Sparks, Halsey G. Knapp, Jr., Krevolin & Horst, LLC, Bruce P. Brown, Bruce P. Brown Law, Cary Ichter, Ichter Davis, LLC, Atlanta, GA, William Brent Ney, Ney Hoffecker Peacock & Hayle, LLC, Lawrenceville, GA, for Plaintiffs.

Baconton Missionary Baptist Church, pro se.

Alexander Fraser Denton, Brian Edward Lake Carey Allen Miller, Joshua Barrett Belinfante, Kimberly K. Anderson, Vincent Robert Russo, Jr., Robbins Ross Alloy Belinfante Littlefield, LLC, Bryan Francis Jacoutot, Bryan P. Tyson, Taylor English Duma LLP, Cheryl Ringer, David R. Lowman, Kaye Woodard Burwell, Office of Fulton County Attorney, Atlanta, GA, for Defendants.

ORDER

AMY TOTENBERG, UNITED STATES DISTRICT JUDGE

I. INTRODUCTION

Approximately two months before the 2018 Georgia state general election, this Court recognized in its first preliminary injunction order that the State had "stood by for far too long" in failing to address the "mounting tide of evidence of the inadequacy and security risks" posed by Georgia's Direct Recording Electronic voting system. *Curling v. Kemp*, 334 F. Supp. 3d 1303, 1307, 1327 (N.D. Ga. 2018). The Court at that time found that Plaintiffs were substantially likely to succeed on the merits of their claims that they faced an imminent threat of the diminishment and burdening of their First and Fourteenth Amendment rights to cast a vote that is properly counted. The Court, however, ultimately determined that the Plaintiffs' eleventh-hour request for an immediate rollout of paper ballots statewide would likely adversely impact the public interest in an orderly and fair election. But, with the 2020 elections looming around the corner, the Court advised the State Defendants that any new balloting system adopted by the State should address democracy's critical need for transparent, fair, accurate, and verifiable election processes that guarantee each citizen's fundamental right to cast an accountable vote. The Court also expressly warned Defendants that further delay by the State in remediating its technologically outdated and vulnerable voting system would be intolerable and any future timeliness objections relating to the State's inability to comply with the requested relief would be of the State's own making.

The State Defendants immediately appealed this Court's denial of their motions to dismiss on jurisdictional grounds and then sought a stay of this case pending the appeal. [1] After the State's appeal was denied in March 2019, the Plaintiffs filed new Motions for Preliminary Injunction. The Plaintiffs' motions seek to enjoin Defendants from using the Global Election Management System ("GEMS") and its central Diebold AccuVote Direct Recording Electronic ("DRE") voting mechanism. The Plaintiffs seek injunctive relief to remedy the claimed unconstitutional gauntlet of state election system practices that continue to thwart and burden their right to vote. And they seek to require the State's use of hand-marked paper ballots in the 2019 municipal and county elections and thereafter. [2] The Plaintiffs also seek equitable relief in connection with the Secretary of State's ("SOS") continued use of an electronic voter registration pollbook system, which they contend is riddled with data reliability and accuracy problems that result in the unconstitutional disenfranchisement and burdening of voters' rights to cast regular ballots that are actually counted.

***2** Plaintiffs' new motions present testimony manifesting a catalogue of pervasive voting problems arising in the 2017-2018 election period that compounds and expands the evidence established in the September 2018 preliminary injunction record compiled before the November 2018 general election, which itself yielded voluminous voting process complaints as well as litigation. Cumulatively, Plaintiffs in this case have marshaled a large body of evidence to demonstrate the burdens to the voting process and to the casting of a secure, reliable, counted ballot that some portion of voters across Georgia, including Plaintiffs, have experienced. The record in this case is substantial. [3]

This case arises in a technology context where Georgia's current voting equipment, software, election and voter databases, are antiquated, seriously flawed, and vulnerable to failure, breach, contamination, and attack. The ongoing breach of the State's Center for Election Systems [4] ("CES") servers, computer networks, and data housed at Kennesaw State University ("KSU"), in 2016 and 2017 unfortunately was an early talismanic event in this saga as was the subsequent wiping of the CES voting system servers upon public exposure of the breach immediately following the filing of this lawsuit. [5] The State Defendants' refusal to fully acknowledge or remedy these circumstances and their broader ramifications for the voting system's security and reliability both before and after the Secretary of State's Office took over the CES's functions has flagged other, similar troubles. [6]

The Court does not minimize the challenges any state faces in operating a secure, reliable voting system in the current cyber era. Still, the Defendants have been slow and poorly equipped in tackling the security and functionality challenges afflicting its current voting system and the well-established deficiencies in a non-auditable DRE voting system. And Defendants' inconsistent candor with the Court about the CES/KSU hack and the security of the servers, as well as other germane subsequent voting system security issues impacts the evidence.

***3** The imminent threats of contamination, dysfunction, and attacks on State and county voting systems, disparaged by the Secretary of State's representatives at the 2018 hearing virtually as a fantasy and still minimized as speculative at the 2019 hearing, have been identified in the most credible major national and state cybersecurity studies and official government reports. And, in "real life," this played out with the United States' July 2018 criminal indictment of a host of Russian intelligence agents for conspiracy to hack into the computers of various state and county boards of election and their vendors as well as agents' efforts during the 2016 election to identify election data system vulnerabilities through probing of county election websites in Georgia and two other states. [7] Similarly, the record demonstrates the perilous vulnerability and unreliability of the State's electronic voter registration system as well as its burdening of Georgia citizens' right to cast a vote that reliably will be counted.

All that said, the posture of the case is also markedly different than in September 2018. The Court concluded in its Order last year that although the Plaintiffs had established a likelihood of prevailing, the balancing of equities and public interest preliminary injunction factors weighed against granting an injunction at that late date because of the magnitude of the administrative and fiscal challenges posed by implementation of a paper ballot system in a statewide election in 2600 precincts and 159 counties. However, the Court forewarned the Defendants that their arguments as to administrative and resource constraints "would hold

much less sway in the future" in post-2018 election cycles "if Defendants continue to move in slow motion or take ineffective or no action." *Curling*, 334 F. Supp. 3d at 1327.

On April 2, 2019, the Governor of Georgia approved newly enacted state election legislation.[8] The legislation replaces the statewide mandated use of DREs with mandated electronic ballot-marking devices ("BMDs") and optical scanners that count votes recorded on the paper ballots produced via printers attached to the BMDs.[9] The legislation also revises various voting procedures and provides somewhat vague requirements for expanded auditing of the balloting system and results, using the ballot printout as a key element in the audit process.

The Secretary of State's Office formally released a request for bid proposals on March 15, 2019, two days after the Georgia Senate approved the legislation. The State represented to the Court that the contract was expected to be awarded by mid-July 2019. Mid-July came and went with no announcement from the State regarding the selection of its voting machine vendor and system. On July 25 and 26, 2019, the Court held a lengthy hearing on Plaintiffs' renewed injunction motions. The hearing concluded after 8:00 p.m. on Friday evening. First thing Monday morning July 29th, the State awarded the low bidder, Dominion Voting Systems, Inc., the contract for a sum of $106,842,590.80. The Secretary of State's contract with Dominion calls for the full implementation of this new voting system in time for Georgia's March 2020 Presidential Preference Primary as well as a pilot of the system in 6 counties in the November 2019 elections. *See Dominion contract and award documents*, available at https://sos.ga.gov/securevoting (last visited August 13, 2019).

***4** The State's response to the current Motions for Preliminary Injunction focused on four themes:

(1) The State contends it has taken substantial proactive, corrective action by passing new election legislation to implement a reliable and secure new election data system based on ballot marking devices, auditable scanned paper ballot printouts, and ballot scanners/tabulators statewide for the 2020 March Presidential Preference Primary.[10] As a result, Defendants further contend that Plaintiffs' request for injunctive relief to bar the use of the DRE system in the 2019 off-cycle elections will cause municipalities and counties to incur significant disruption and financial burdens to implement a hand-marked paper ballot system in a single election cycle in 2019 and such disruption is far outweighed by the important, pragmatic operational challenge of progressive training on and rollout of the new BMD based voting system and pollbooks in the next few months prior to the Presidential Primary.

***5** (2) The State contends it has made progress and taken adequate measures to fortify and address the security and vulnerability of the election data system.

(3) The State contends that all voting systems have their own risks and that Plaintiffs' experts' assessment of the risks (or dangers) of the State's continued use of the DRE/GEMS system and database in the current security environment is unsubstantiated or overstated.

(4) The State contends that all municipalities with scheduled elections in the Fall of 2019 are necessary parties and that the Court cannot proceed to consider the requested relief without these municipalities being joined as party-defendants in these proceedings.

The Coalition and Curling Plaintiffs, by contrast, argue that the State's use of the DRE/GEMS system will likely continue past March 2020, which the State has set as its target for implementing the new BMD/scanner based voting system – whether because this target date is not likely to be met or because of other system deficiencies or defects that will continue onward. They further argue that voters should not be forced anew to run the gauntlet of a voting system in which their ability to cast votes that are properly counted is compromised or thwarted. They thus seek a hand-marked paper ballot system, with appropriate risk limiting auditing and other measures that are consistent with the recommendations of leading cybersecurity election experts and feasible based on the experience of other state and county jurisdictions that have implemented hand-marked paper ballot based voting systems.

This Opinion and Order begins by rejecting the State Defendants' Rule 19 joinder argument. With that issue out of the way, the Court then details the record evidence demonstrating the serious and continuing vulnerabilities in the State's current electronic voting system that burden the Plaintiffs' constitutional rights. The Court also recounts the mountain of voter testimony showing that these vulnerabilities have a tangible impact on these voters' attempts to exercise their fundamental right to cast a ballot and have their vote counted. The Order further addresses the evidence from both parties regarding the feasibility of implementing Plaintiffs' requested relief of hand-marked paper ballots in the 2019 elections, especially in light of the State's newly enacted BMD voting system. Finally, the Court considers the totality of this evidence and the established legal standards in weighing whether to grant Plaintiffs' requested relief.

Based on this careful review of the record, and consideration of the relevant factors for granting injunctive relief, the Court **GRANTS IN PART** and **DENIES IN PART** the Plaintiffs' Motions for Preliminary Injunction [Doc. 387 and Doc. 419].

II. JOINDER OF MUNICIPALITIES CONDUCTING NOVEMBER 2019 ELECTIONS

The State Defendants assert that Plaintiffs lack standing to obtain the relief sought because "State Defendants have no control over the upcoming municipal elections" and therefore "any injunctive relief against State Defendants would not achieve Plaintiffs' desired results." (Resp., Doc. 472 at 12-13.) According to the State, each of the Georgia municipalities that conduct their own elections are necessary parties and Plaintiffs' failure to join them in this suit precludes relief under Federal Rule of Civil Procedure 19.

***6** This Court has previously rejected variations of this argument in its prior Orders on the Defendants' Motions to Dismiss. For example, Defendants argued that an injunction prohibiting the State Defendants from using DREs would not actually stop the deployment of DREs because the State is not the entity that enforces the law requiring DREs and county officials not included in this suit would continue to use DREs. Recall that this Court found: (i) the State Defendants play a critical role in directing, implementing, programming, and supporting the DRE system throughout the State, (ii) the Secretary of State has the authority and obligation under Georgia law to take appropriate corrective action in connection with the continued use of the DRE system, and (iii) the State Defendants are in a position to redress the Plaintiffs' injury because the requested injunctive relief as to the suspended use of the DRE voting system would enjoin both the State Defendants as well as counties required to use the DREs, including the Fulton County Defendants. [11] *See Curling v. Kemp*, 334 F. Supp. 3d 1303, 1318 (N.D. Ga. 2018).

More recently, in a related challenge to Georgia's election system, *Fair Fight Action Inc. v. Raffensperger*, Civil Action 1:18-cv-5391-SCJ, fellow District Court Judge Steve Jones found that "county election officials are not necessary parties under Rule 19(a)(1)(A) because this Court can provide 'complete relief' among the current plaintiffs and defendants without joining the counties in that existing defendants have the statutory oversight ability to enforce uniform and state-wide election standards and processes." (Order, Doc. 68 at 63) (citing *Grizzle v. Kemp*, 634 F.3d 1314 (11th Cir. 2011) (finding that while the Secretary of State cannot directly perform certain acts that are ordinarily performed by the counties, "as a member and the chairperson of the State Election Board, he has both the power and the duty to ensure that the entities charged with those responsibilities comply with Georgia's election code in carrying out those tasks ... his power by virtue of his office sufficiently connect[s] him with the duty of enforcement....") and Ga. Op. Att'y Gen. No. 2005-3 (Apr. 15, 2005) (recognizing the Secretary of State's authority to manage the State of Georgia's electoral system and the oversight duty of the State Election Board)). [12] In addressing the State's assertion that "it would be inequitable to issue an order compelling the spending of county resources – local taxpayer dollars – without bringing the counties into the lawsuit," Judge Jones reasoned that "the fact that there may be some type of indirect cost to the counties in having to comply with the law is not the test at this point, as the focus of the Rule 19(a)(1)(A) analysis is whether the Court can provide complete relief among the parties presently in the case." (Order, Doc. 68 at 63-64.) He further found that absent the assertion of an interest in the case by any county, the State's argument was not relevant to the Court's joinder determination under Rule 19. The court's Rule 19 analysis in *Fair Fight Action* is persuasive and the reasoning is sound.

"The purpose of Rule 19 is to 'permit joinder of all materially interested parties to a single lawsuit so as to protect interested parties and avoid waste of judicial resources.' " *Askew v. Sheriff of Cook Cty., Ill.*, 568 F.3d 632, 634 (7th Cir. 2009). In determining whether a party is "necessary" or "indispensable" under Fed. R. Civ. P. 19, the Eleventh Circuit provides the following guidance:

> ***7** Rule 19 provides a two-part test for determining whether an action should proceed in a nonparty's absence. The first question is whether complete relief can be afforded in the present procedural posture, or whether the nonparty's absence will impede either the nonparty's protection of an interest at stake or subject parties to a risk of inconsistent obligations. *See* Fed. R. Civ. P. 19(a)(1)-(2). Only if we can answer this threshold question "yes," and if the nonparty cannot be joined (say for jurisdictional reasons), do we go to step two. *See Temple v. Synthes Corp., Ltd.*, 498 U.S. 5, 8, 111 S.Ct. 315, 112 L.Ed.2d 263 (1990). Step two asks us to determine, "in equity and good conscience," whether the action should go forward as cast. *See* Fed. R. Civ. P. 19(b). The Rule provides us four factors to consider. *See id.*; *see also Laker Airways, Inc. v. British Airways, PLC*, 182 F.3d 843, 848 (11th Cir.1999). The Supreme Court has instructed us in this step-two analysis to eschew formalism in favor of flexible practicality. *See Provident Tradesmens Bank & Trust Co. v. Patterson*, 390 U.S. 102, 118–19, 88 S.Ct. 733, 19 L.Ed.2d 936 (1968).

City of Marietta v. CSX Transp., Inc., 196 F.3d 1300, 1305 (11th Cir. 1999). "The 'complete' relief concept of Rule 19(a)(1) 'refers to relief as between the persons already parties, not as between a party and the absent [party] whose joinder is sought.' " *Heinrich v. Goodyear Tire & Rubber Co.*, 532 F. Supp. 1348, 1359–60 (D. Md. 1982) (citations omitted). In making this determination, "pragmatic concerns, especially the effect on the parties and the litigation, control." *Focus on the Family v. Pinellas Suncoast Transit Auth.*, 344 F.3d 1263, 1280 (11th Cir. 2003); *accord Challenge Homes, Inc. v. Greater Naples Care Ctr., Inc.*, 669 F.2d 667, 669 (11th Cir. 1982).

The State Defendants previously argued in filings before the Court that preceded Plaintiffs' renewed preliminary injunction motions that the Secretary of State plays a limited role in both county and municipal elections. (*See* Doc. 367.) In response to Plaintiffs' motions for immediate relief in time for the Fall 2019 elections, the State Defendants have scaled back their objection, focusing on municipalities only. The State Defendants now appear to recognize that counties have no leeway in how to conduct their elections under Georgia's election code, despite their prior contradictory assertion that "municipalities *and counties* have authority to determine ... the method of said elections ..." (Doc. 367 at 2) (emphasis added). *See also* O.C.G.A. § 21-2-300 ("The equipment used for casting and counting votes in county, state, and federal elections shall be the same in each county in this state and shall be provided to each county by the state, as determined by the Secretary of State."). As the counties are required to use the same equipment as the State is required to use, Defendants do not argue, and there is no basis to conclude that any relief ordered against the State as to the required method of voting in future elections will not be enforceable against Georgia's counties.

In contrast, Georgia's municipalities are not subject to the uniform statewide voting equipment requirement, though many municipalities contract with their county to conduct the municipal elections using the county equipment. "When municipalities contract with their county to conduct the municipal elections, the State Defendants perform the same actions as if the election were a county, state, or national election." [13] (State Defs.' Resp. to Court Order for information regarding scope of 2019 elections, Doc. 537 at 2.) According to the most recent information provided on July 25, 2019 by the State Defendants, there are 386 scheduled elections for Fall 2019: 12 countywide elections; 275 municipal elections run by counties; and 99 municipal elections run by municipalities. All 287 county-run elections are conducted on DREs. Of the 99 municipality-conducted elections, 70 are conducted on hand-marked paper ballots (tabulated by optical scan or hand count), 23 are conducted on DREs, and six are conducted with lever machines. [14]

***8** Contrary to the State Defendants' assertion that complete relief cannot be afforded without joinder of the municipalities, the Secretary of State is the chief election official. Georgia law confers primary authority on Georgia's Secretary of State to manage Georgia's electoral system. *See* O.C.G.A. § 21-2-50(b); *see also* Ga. Op. Att'y Gen. No. 2005-3 (Apr. 15, 2005) ("[I]it is clear that under both the Constitution and the laws of the State the Secretary is the state official with the power, duty, and authority to manage the state's electoral system...."). The Secretary of State and State Election Board also have significant statutory oversight authority to train local elections officials, set election standards, and investigate failures of local elections officials. *See* O.C.G.A. § 21-2-31; O.C.G.A. § 21-2-50(a)(11)). Section 21-2-50(a) of the Georgia election code prescribes the powers and duties of the Secretary of State, and requires the Secretary of State to "develop, program, build, and review ballots for use by counties and municipalities on voting systems in use in the state." O.C.G.A. § 21-2-50(a)(15). Section 21-2-379.4(d) provides that "[t]he form and arrangement of ballots shall be prescribed by the Secretary of State and prepared by the election superintendent." O.C.G.A. § 21-2-379.4. The undisputed evidence in this case is that the Secretary of State's office (and in many or most instances its vendor ES & S [15]) builds the electronic ballots for use on DREs using the GEMS software, database, and server. However, the State Defendants have represented that a municipality may "work with a third-party vendor to build its own ballot." (Doc. 537 at 2.) The Court directed the State Defendants to identify these municipalities, but they failed to do so. (*See id.*) By allowing a municipality to contract with a third-party vendor to program and build ballots, the Secretary of State appears to run afoul of its statutory obligations under Georgia's election code (but in any event has implicitly approved the arrangements made by such municipalities for the 2019 elections).

In response to an inquiry from the Court in April of 2019 regarding the scope of the anticipated 2019 elections, the State Defendants contended that they "anticipate[d] that municipal officials will seek to be heard by the Court on any potential injunctive relief for 2019 and should be heard because of their interest in this case." (Doc. 362 at 10.) No municipalities have moved to intervene for this limited purpose. The State Defendants presented with their response brief a handful of declarations from *county* election officials regarding the feasibility of implementing a change to paper ballots in advance of the Fall 2019 elections. State Defendants presented no evidence from any of the municipalities that conduct their own elections on DREs regarding the burden of switching to a paper ballot system before the scheduled elections. [16]

***9** The Court finds that joining all of Georgia's counties and municipalities into this action is not feasible and is not required to provide relief to Plaintiffs where the State's Chief Election Officer charged with implementation and enforcement of the State's election system is a party. [17] *See* O.C.G.A. § 21-2-50(b) (referring to the Secretary of State as "the state's chief election official"). Defendants are not advocating that the Court needs to join the Georgia counties to provide relief as requested by Plaintiffs, therefore admitting they are not necessary parties under Rule 19. Despite their generalized and hyperbolic arguments regarding the need to join municipalities, the evidence shows that: (i) 275 of the 386 scheduled municipal elections are conducted by the counties; (ii) 70 of the 99 municipality-conducted elections are conducted on hand-marked paper ballots as Plaintiffs requested and six (6) are conducted using lever machines; and (iii) 23 of the 99 municipalities will conduct elections using DREs. The State Defendants have presented no evidence regarding which of these municipalities rely on the Secretary of State to build their electronic ballots, which contract with a third-party vendor to build the ballots, or which, if any, may build their own ballots. Georgia law requires the Secretary of State "[t]o develop, program, build, and review ballots for use by *counties and municipalities* on voting systems in use in" Georgia. O.C.G.A. § 21-2-50(a)(15) (emphasis added). Therefore, if the Secretary of State is enjoined from preparing electronic ballots and ordered to provide only paper ballots for use by counties and municipalities (and to procure optical scanners/tabulators pursuant to O.C.G.A. § 21-2-300 for use as needed), Plaintiffs would be afforded complete relief. Accordingly, the evidence, coupled with the State Defendants' duties and responsibilities under Georgia law to oversee, implement, and manage all primary and general elections in the State, compels a finding that joinder of the 23 municipalities is not required under Fed. R. Civ. P. 19.

III. CONTINUING VULNERABILITY AND UNRELIABILITY OF GEORGIA'S GEMS/DRE SYSTEM AND VOTER REGISTRATION SYSTEM AND DATABASE

A. Georgia's DREs operate on outdated and vulnerable software.

The 2000 presidential election spurred the national transition from mechanical to electronic voting machines and from manual to automated processes. National Academies of Sciences, Engineering, and Medicine, et al. *Securing the Vote: Protecting American Democracy* at 109 (National Academies Press, 2018) ("National Academies Report" or "NAS Report"). In 2002, Congress passed the Help America Vote Act ("HAVA") and authorized the allocation of $3 billion to the states, primarily for the purchasing of new voting technology. [18] As a result, federal funding pursuant to HAVA led to the development and deployment of new voting machines, and in particular, a more widespread deployment of DRE devices. (*Id.*) While HAVA provided necessary funding for improved voting technology, contemporaneous with the Act's passage, available voting technologies had existing security and operational flaws. (*Id.* at 110.) For example, "DRE machines did not produce a means for voter verification." (*Id.*)

HAVA contained no provisions for future funding of replacement voting machines or updates to the system. (*Id.*) Consequently, in 2018 the National Academies of Science concluded:

> [t]he depletion of the HAVA funds has significant implications today, as the systems deployed as a result of HAVA are nearing the end of their useful life and need to be replaced. The service life of most new voting hardware and software purchased and installed immediately after the passing of HAVA is 10-15 years, and states now lacking HAVA funds have to go to extraordinary lengths to keep their aging systems operational.

***10** (*Id.*)

Georgia's DRE system originally was intended to include the capacity for an independent paper audit trail of every ballot cast, but this feature was never effectuated. (Report of the 21st Century Voting Commission, Pl. Ex. 10 at 38, introduced at Preliminary Injunction hearing; testimony of Cathy Cox.) In the September 2018 hearing, former Secretary of State Cathy Cox testified that when Georgia made the switch to DREs without the option for a paper trail in 2001, "none of us contemplated that this would be the end of the process but that it would – that Kennesaw to some extent could help us stay on top of things. But I don't know that we realized this equipment probably could not be updated as much as we would have anticipated. We probably didn't anticipate obviously a recession would come about and there wouldn't be money to provide new equipment over time." (Tr., Doc. 307 at 293-94.)

Georgia chose to use the Diebold Accuvote DRE which relies upon versions of Windows and BallotStation software (developed in 2005) both of which are out of date – to the point that the makers of the software no longer support these versions or provide security patches for them. (Halderman Decl., Doc. 260-2 ¶¶ 24-28.) As Dr. Halderman [19] testified, the DREs use "a Windows CE operating system that is notoriously insecure. It doesn't have a security subsystem, for example." (Tr., Doc. 307 at 137.) The operating system software on Georgia's DRE machines has not been updated since at least 2005 to address any of the security flaws discovered in the software over the last 13 plus years. (Halderman Decl., Doc. 260-2 ¶¶ 27-28.)

In 2006 Harri Hursti, [20] a nationally recognized cyber expert and "ethical hacker," discovered a serious vulnerability in the AccuVote TSX – the same model of DRE machines used in Georgia. The State Defendants' own retained expert described this vulnerability in the AccuVote DREs as "one of the most severe security flaws ever discovered in a voting system," up to that time. (Shamos Dep. at 115.) Hursti's 2006 security alert report demonstrated numerous vulnerabilities with the AccuVote TSX, the most critical security issue being that the machine's operating software enables "a malicious person to compromise the equipment even years before actually using the exploit, possibly leaving the voting terminal incurably compromised.... [The] defects compromise the underlying platform and therefore cast a serious question over the integrity of the vote. These exploits can be used to affect the trustworthiness of the system or to selectively disenfranchise groups of voters through denial of service." Harri Hursti, *Diebold TSX Evaluation, Security Alert: May 11, 2006, Critical Security Issues with Diebold TSX*, Executive Summary at 2. [21]

***11** After Hursti's security alert was issued, Diebold was forced to create a security patch for the vulnerable TSX software. There is no evidence that Georgia ever implemented the software patch or made any upgrades to protect the integrity of its DRE machines. (Shamos Dep. 116-17.) Georgia's AccuVote DRE machines use software from at least 2005, which predates the version of the software released by Diebold after the Hursti discovery in 2006 and the updated BallotStation software on the same model Diebold Accuvote TSX machines that were decertified in California in 2006-07 as discussed below. (*See* Halderman Decl., August 2018, Doc. 260-2 ¶ 25.) Michael Barnes, Director of the Center for Election Systems at the Secretary of State's office, testified that the internal memory of the DRE voting machines themselves has never been tested or inspected by the State. (Tr., Doc. 570 at 77.)

B. The DREs work in tandem with the Global Election Management System ("GEMS") interface, which poses additional problems for election integrity and security.

The DREs work in tandem with the Global Election Management System ("GEMS") – the computer software that generates the ballot programming files. [22] (Halderman Decl. ¶ 31) (stating that the computer software that generates the ballot programming files is called an election management system (EMS)). According to Dr. Halderman, "ballot programming files typically are created by election officials either on a regular desktop computer in a government office, or by an election service vendor that creates programming for voting machines across many jurisdictions." (Halderman Decl. ¶ 31; *see also* Tr., Doc. 570 at 60-61 (Merritt Beaver's testimony describing the ballot building process and files being moved back and forth from desktop computers to the GEMS server and vice versa).) Michael Barnes, Director of the CES, is responsible for oversight of the GEMS ballot generation files for all 159 Georgia Counties.

The Georgia GEMS server runs on a Windows XP/2000 operating system. [23] (Tr., Doc. 307 at 227, 307-308; Tr., Doc. 570 at 274-75.) In general terms, as explained more fully below, the ballots are constructed in a GEMS database at the State level, the ballot database is transmitted to the Counties, and then transferred onto memory cards that load the ballots into the DRE voting machines. At the end of the election, the election data from the memory cards is then uploaded onto the County GEMS server that tabulates the county election votes. [24] Thus, in addition to serving as the ballot building platform, the GEMS system also serves as a means of communication/transmission of ballot and voting data downloaded to and from the DREs and between the County and State GEMS servers. Because of the interface between the GEMS and the DREs, an infection or intrusion in the GEMS system ballot programming files can spread viruses and malware from the GEMS to all voting machines serviced by GEMS. (*See* Halderman Decl. ¶ 31.) As described below, a malware or virus attack can occur at any level here (the ballot programming files, DRE removable memory cards, or GEMS database at the County or State level.) (*Id.* at ¶ ¶30-32.)

***12** The testimony of CES Director Michael Barnes about the GEMS system has been inconsistent. At the September 2018 injunction hearing he testified that, "[w]e have an air gapped system within the Secretary of State's office that holds our ballot-building information, our ballot-building software. And that is the system that is used to produce that data output." (Tr., Doc. 307 at 207.) He testified the system containing the "ballot-building software" is never connected to the internet. (*Id.* at 207-208.) He even stated that "[t]he SOS server where the ballot-building information is housed today – I don't even have access to that server. It is within a locked environment that only the IT systems operators for the Secretary of State's office have access." (*Id.* at 208.) [25] Barnes testified that the "only thing that is used to transfer data from the private network over to distribution points is a single USB – lockable USB drive ... used to take PDF files that are generated as proofs to transfer over for county for proofing purposes." (*Id.* 227-28.) Barnes connects the USB drive to his public internet-facing computer that "is connected to a secure FTP [file transfer protocol] site." (*Id.* at 228.) But he also stated that the "GEMS server within the Secretary of State's office that I do my work on does not have a wireless connect point," which is the basis for his understanding that "it is a secured air gapped system." [26] (*Id.* at 226.)

During the July 2019 hearing, Barnes described the GEMS ballot building process differently than how he portrayed the process in September 2018. The ballots are not built on the private GEMS server in the Secretary of State's secure facility. (Tr., Doc. 570

at 166-67.) The ballots are built on the GEMS application (the "ballot-building software") on public-facing internet-connected desktop computers of the individual ballot builders, then copied over from the public-facing computer onto a "lockable" USB drive, which is then inserted into the private [27] computer to be uploaded into the secure GEMS server for storage of the ballot programming files. (*Id.* at 77-78, 166-67.) Mr. Barnes scans and reformats the lockable USB drive during each transfer. (*Id.* at 77-78, 101, 107.) He follows the same process when copying files from the private GEMS server to the USB drive and back onto the public internet-facing computer for distribution to the counties. (*Id.* at 101, 107.)

The Secretary of State has contracted with ES & S for ballot building support services to "assist" the Center for Election Systems in constructing the GEMS databases that are used within county elections. (*Id.* at 83-84.) Three individuals from ES & S [28] work solely on Georgia election databases and perform "their ballot building work within their own purviews" and construct the GEMS databases on desktop computers from their homes. (*Id.* at 84-85.) According to Barnes, the individuals are subject to the same requirements for using air gapped equipment as the Secretary of State, though he testified he does not know what physical security parameters each of the individuals have within their homes. (*Id.* at 85-86.) These individual contractors built all of the ballots for all counties for the November 2018 general election, and they built the ballots for 98 out of 159 counties for the May 2018 primary election. (*Id.* at 174.)

***13** Once the State collects all of the information from the counties relating to candidates, jurisdictions, and races involved in the election, the three individual contractors construct the initial GEMS databases and initial layout of the data set. (*Id.* at 162.) The databases are then delivered to the SOS on an encrypted CD or locked USB drive. (*Id.* at 163.) Barnes "moves the files from their thumb drives into" the State's GEMS file system by downloading the data on the public computer and then onto his lockable reformatted USB drive that he "uses for moving the files back and forth" from his public and private/air-gapped computers. (*Id.* at 164-65.) The GEMS server holds the ballot file, which is then placed into a review folder on the server for inspection. (*Id.* at 165.) Barnes and his staff perform a "line-by-line review of the data set to make sure that the right candidates are listed in the right order, names are spelled properly, [and] that the races are in the proper order." (*Id.* at 163.) If any corrections are needed on the contractor-built GEMS ballot databases, they are not returned to the contractors. Instead, Barnes or his staff make those corrections. (*Id.* at 163-64.)

Barnes described this review/correction process as follows:

> A. Once the file is placed into a review folder on the server, then a member of my team – we have a check sheet that is itemized of what we're looking at that is within a specific database within specific elections. They will then download from the server a copy of that file. And it is saved to their local private CPU. The local – private CPU is where the GEMS executable application or the GEMS application is residing. The GEMS application is not residing on the server. It is just – the server is just holding files. The GEMS application is on the individual's own CPU. They download a copy of that file onto their computer. They open up the data file on their computer. And they begin examining it to make sure that it has been built properly, that all precincts are there, all district combinations – that all ballots are there, all voting locations. That everything has been built properly.
>
> Q. All right. So then if they make a correction because somebody's name has been spelled incorrectly or for whatever reason, they save it again on that. What happens then?
>
> A. Right. They first – after they have made the correction, the corrected file is residing on their personal CPU. They then create a backup copy of that file and save it back to the server. That saving action back to the server replaces the existing copy with the modified copy. So we only have one copy of the database sitting on the server.
>
> Q. Is that the public server, or is that on your –
>
> A. That is the private.
>
> Q. That is the private, your units?

A. Yes. Everything constructed with the GEMS is done through the private environment.

Q. All right. So then what happens?

A. Then it moves from a review – a review of the database function. Then the file is moved from one folder to another folder. That folder is for audio and visual inspection. Once it is placed into that folder, we have a dedicated room in our office where a member of my team will go in, again copy that file from the server onto a private CPU in order to create an election media, a memory card that is then placed into a touchscreen device within that room. And then we look at the ballot on a DRE to again validate that all the races are appearing, all the candidates are in the proper order, that all the audio files are in place, that we do not see any – any issues with the display of the ballot on the touchscreen. Sometimes because of long questions or such, the screen doesn't look correct in the way it lays things out. So that would make us then make some subtle scaling adjustments in the display of the database, which requires us to touch the database again.

(*Id.* at 165-67.) This is entirely contrary to the following testimony Mr. Barnes gave to this Court in the September 2018 hearing, just shy of two months prior to the November election:

Q. Do state workers type in every race and candidates' name into the GEMS server?

***14** A. Yes, sir.

Q. So that is how the data gets loaded?

A. Yes, sir. It is all manual entry.

(Tr., Doc. 307 at 226-27.) Despite his testimony in September 2018 that the entire ballot building process is done in-house on a secure GEMS server, the ballot programming was not done by state staff by manual entry directly into the GEMS server housed in the State's secure facility.

Finally, once counties approve the ballot proofs and ballot database reports, CES provides each county with a single CD with a single file that is the County GEMS database. (Tr., Doc. 570 at 170.) The county takes the CD that contains its GEMS database, loads it into their local GEMS computer and creates the various media they use (*i.e.* memory cards) to program and power the DRE and optical scan units. (*Id.*) Election results data from the DRE machines is stored on the memory cards that is transferred back to the County GEMS server for tabulation of results that are subsequently relayed to the Secretary of State both via the Election Night Reporting System and later manual delivery of a CD.

Dr. Halderman was surprised to learn that the Secretary of State's Center for Election Systems uses outside contractors working from their home computers to build Georgia's ballots for use on the DREs. (Tr., Doc. 571 at 87.) These computers that the contractors are working on in their homes are outside the secure facilities that the Secretary of State maintains for ballot building. (*Id.*) The ballot files must be transmitted into the secured facility on USB drives, and the data from those drives is then copied by Mr. Barnes through his public internet-connected computer [29] in order to transfer them into the separate/private secure GEMS server. (*Id.*) Thus, the election programming for every county that is programmed by those external contractors, which included every county in Georgia during the November 2018 general election, travelled through an internet-connected computer where there is an attendant risk of infection by malware that can then be spread to voting machines. (*Id.*)

As Dr. Halderman testified, the process that Barnes described using to transfer GEMS files using a “lockable” (presumably a write-protect switch) USB drive is not in fact secure and does not protect the integrity of the GEMS system as portrayed by Mr. Barnes and Mr. Beaver. (*Id.* at 88.) In order to move the files between the USB drive and the computers, Barnes “has to have [the USB] unlocked in his internet-attached computer in order to format it in order to copy files to it.” According to Halderman, this process unfortunately exposes the data to infiltration by new malware (or other modes of tampering with election software or data) that can then contaminate the entire election system. (*Id.*)

C. The DRE/GEMS system is particularly susceptible to manipulation and malfunction.

In connection with their 2018 preliminary injunction motions, Plaintiffs presented considerable evidence that Georgia's outdated DRE voting system is highly susceptible to manipulation and malfunction. As Plaintiffs' expert, Dr. Alex Halderman testified here (and most recently before the U.S. Senate Select Committee on Intelligence), Georgia's DRES are vulnerable to various routes of infection and attack that are difficult or impossible to detect or reverse. (Halderman Decl., Doc. 260-2.) They include the following: A computer virus could subtly steal votes from one candidate and assign them to another, without detection. A malicious intruder could install malware that would alter the vote count or stop the machine from accepting votes, as demonstrated during the 2018 injunction hearing. [30] Anyone with access to a single voter access memory card, could spread malware from the card to DREs and then from DREs to the election management system, potentially infecting the entire voting system. An attacker can access the ballot programming files on an unsecure election management system and piggyback on the pre-election programming process to spread malicious software to the voting machines across all jurisdictions serviced by the GEMS system. And as Dr. Halderman demonstrated in April 2018, Diebold DRE machines can be hacked remotely to steal votes, a method by which foreign adversaries could impede elections without any physical access to voting machines. (*Id.* ¶ 26, n. 20.)

***15** Other cybersecurity elections experts have shared in Dr. Halderman's observations of the data manipulation and detection concealment capacity of such malware or viruses, as well as the ability to access the voting system via a variety of entry points. (*See* DeMillo Decl., Doc. 277, Ex. C; *see also* DeMillo Suppl. Decl., Doc. 548 at 75-85 (supplementing his prior expert testimony in connection with 2018 preliminary injunction motion discussed in 2018 Order regarding observation of malfunction of DRE machines and Express Pollbooks during 2018 election); [31] Buell Decl., Doc. 260-3; Stark Decl., Doc. 296-1; Lamb Decl., Doc. 258-1 at 126-135; *see also* Bernhard Decl., Doc. 258-1 at 33-42.)

Dr. Halderman and Dr. DeMillo also explained in their testimony in detail the reasons why the DRE auditing and confirmation of results process and parallel testing of DREs used by state officials on a restricted sample basis is of limited value. (Halderman testimony at hearing; Halderman Decl., Doc. 260-2 ¶¶ 35-48; *see also* DeMillo Decl., Doc. 277, Ex. C ¶¶ 10-20.)

This evidence was buttressed by a mounting tide of research and testing by the nation's leading election cybersecurity experts in election cybersecurity. The consensus of these experts, recently reaffirmed by the National Academies of Science, Engineering and Medicine and the U.S. Senate Select Committee on Intelligence reports in September 2018 and July 2019 respectively, has reached national prominence in the general public's understanding of election security. As the Amicus Brief of the Electronic Privacy Information Center discusses, almost from their inception, DREs have been plagued by warnings that the voting machines are unreliable, insecure, unverifiable. [32] As the evidence presented by Plaintiffs in this case shows – while Georgia election officials have effectively taken no steps to address these deficiencies with its DRE-based system – a litany of other states have abandoned the plagued machines in exchange for a more secure and reliable alternative voting method. *See Election Assistance Comm'n, Overview of Election Administration and Voting in 2018* 20 (Jun. 27, 2019). These include California, Colorado, Kansas, Kentucky, Ohio, and Virginia. (Doc. 437-2 at 10-12.)

***16** Plaintiffs' expert, Dr. Alex Halderman was part of an expert team of computer scientists who conducted the "top to bottom" review of California's DRE system in 2006, which concluded that the machines were "inadequate to ensure accuracy and integrity of the election results." (Halderman Decl. ¶ 22, Doc. 260-2.) This report informed the California Secretary of State's decision to decertify the machines and transition to a paper ballot system. (*Id.*)

The Court has also considered the Declaration and hearing testimony of Lowell Finley, former Deputy of State for voting Systems Technology and Policy (and simultaneously general counsel for 3 years) for the State of California for the period 2007-2014. Mr. Finley oversaw California's top-to-bottom review of the state's electronic voting systems that included computer security experts from major universities including Stanford, University of California, Princeton, and Rice. "The review resulted in the de-certification of several DRE systems, including a version of the AccuVote TSX currently used in Georgia based

primarily on severe security vulnerabilities uncovered during the review." (Doc. 387-3 at 3.) And Mr. Finley oversaw the rollout in dozens of California counties of paper, hand completed ballot systems including optical machine scanning and tabulation along with a verifiable paper audit trail. (*Id.*; *see also*, Declaration of Nathan Woods, Doc. 510-2.)

Similarly, Candace Hoke, who offered testimony in support of the Coalition Plaintiffs' preliminary injunction motions (discussed more fully below in Section IV), was part of a team of election security experts advising Ohio's Secretary of State Jennifer Brunner in 2007 regarding vulnerabilities in its DREs. Secretary Brunner's Evaluation and Validation of Election-Related Equipment, Standards and Testing ("EVEREST") initiative – which examined a newer version of the AccuVote DREs than Georgia uses – found that vulnerabilities in the voting system's security and reliability were easily exploitable by an attacker under election conditions. Secretary of State Jennifer Brunner, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing* (Dec. 2007) at 103. Following the report, the Ohio Legislature eliminated Ohio's electronic voting machines.

In their 2019 preliminary injunction submissions, Plaintiffs offer additional declarations from other prominent cybersecurity election technology experts. Additional expert declarations filed and testimony of note considered here came from Dr. Andrew Appel, the Eugene Higgins Professor of Computer Science at Princeton University, where he served as Department Chair from 2009-2015. Dr. Appel has also served as both the Director of Undergraduate Studies and Director of Graduate Studies and as Editor in Chief of ACM Transactions on Programming Languages and Systems, the leading journal in his field, and he is a fellow in the Association for Computing Machinery, the leading scientific and professional society in Computer Science. In 2017, Dr. Appel was appointed by the National Academies of Science, Engineering and Medicine to serve on the Consensus Committee on the Future of Voting, inclusive of computer scientists, election officials, and other subject matter experts and was chaired by two university presidents, one a computer scientist and one a law professor.[33] Dr. Appel has also testified on election technology before the U.S. House of Representatives and the New Jersey legislature as well as in other proceedings. (Doc. 510-2.)

***17** The National Academies of Sciences Report issued in September 2018, in which Dr. Appel participated, concerning the integrity of voting systems and the risks associated with digital technology, determined:

> [A]ll digital information – such as ballot definitions, voter choice records, vote tallies, or voter registration lists – is subject to malicious alteration; there is no technical mechanism currently available that can ensure that a computer application – such as one used to record or count votes – will produce accurate results; testing alone cannot ensure that systems have not been compromised; and any computer system used for elections – such as a voting machine or e-pollbook – can be rendered inoperable.

National Academies of Sciences, Engineering, and Medicine, et al. Securing the Vote: Protecting American Democracy 42, 80 (National Academies Press, 2018) ("National Academies Report" or "NAS Report"). The NAS report identified several risks and usability problems with DRE voting machines. (*Id.* at 78.) The advent of DREs in the early 2000s introduced "new technical challenges," such as touchscreen miscalibration, which causes a voter's intended selection of one candidate to be misinterpreted as a vote for another candidate. (*Id.*) However, the NAS was even more concerned about the risk of undetectable cyberattacks on DREs that lack a "paper artifact that could be manually counted." (*Id.*) Furthermore, the NAS report emphasized that any voting system should allow a voter to verify that the recorded ballot reflects his or her intent, which isn't possible with paperless DRE machines. Although some concerns with DREs are alleviated if the machines create voter verified paper audit trails (VVPATs), the NAS report notes that "it is possible that the information stored in a computer's memory does not reflect what is printed on the VVPAT." (*Id.*) The NAS also endorsed the use of "risk-limiting audits," in which individual randomly selected paper ballots are examined until sufficient statistical assurance is obtained. (*Id.* at 95.) The key to the NAS recommendation is that paper ballots are required for such audits. The report recommended that voting machines that do not produce paper audit trails "be

removed from service as soon as possible" and that "[a]ll local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election." (*Id.* at 80.)

The NAS report also noted several cybersecurity risks regarding electronic pollbooks and voter registration databases. It detailed concerns about "unauthorized access to or manipulation of the registrant list" because voter registration databases are "often connected, directly or indirectly, to the Internet or state computer networks." (Doc. 285-1, Ex. 1 at 57.) As an example of the vulnerability of electronic voter databases, the report listed the server error that left 6.5 million voter records in Georgia exposed for six months in 2016-17. (*Id.* at 58.) The NAS report listed a number of ways in which cyberattacks on electronic voter registration data or e-pollbooks could disrupt elections: 1) by altering voter registration databases used to generate pollbooks; 2) by altering the record of which eligible voters have actually voted; and 3) by a "denial-of-service" attack, which would shut done voting altogether. (*Id.* at 72.) Thus, the NAS report recommends that "[j]urisdictions that use electronic pollbooks should have backup plans in place to provide access to current voter registration lists in the event of any disruption." (*Id.*)

***18** Dr. Halderman most recently testified before the U.S. Senate Select Committee on Intelligence that prominently featured his testimony in its report, 2016 U.S. Election, Vol. 1: Russian Efforts Against Election Infrastructure with Additional Views, 116th Cong., 1st Session (2019) (*partially redacted*) ("SSCI Report"). The Senate Select Committee on Intelligence concurred with the NASEM regarding the susceptibility of electronic voting machines to external manipulation in its report on Russian interference in the 2016 U.S. election. [34] Relying on testimony from Dr. Alex Halderman and other experts, the SSCI noted that "researchers have repeatedly demonstrated that it is possible to exploit vulnerabilities in electronic voting machines to alter votes." (SSCI Report at 40.) A computer virus could steal votes from one candidate and assign them to another or could stop the machine from accepting votes altogether. (*Id.*) According to the Senate Committee report, DRE machines "can be programmed to show one result to the voter while recording a different result in the tabulation." (*Id.* at 42.) Therefore, the SSCI report called for states to discontinue using DREs, which "are now out of date." (*Id.*)

The Senate Committee further echoed these findings regarding voter registration systems. After holding hearings, reviewing intelligence, and hearing testimony from state election officials and U.S. Government authorities responsible for election security, the Committee also concluded that voter registration databases and electronic pollbooks, which can be accessed over the internet, are vulnerable components of U.S. election infrastructure. (SSCI Report at 57.) The July 2019 SSCI report noted that Russian government cyber actors engaged in operations to scan the election-related state infrastructure of all fifty states and conducted research on "general election-related web pages, voter ID information, election system software, and election service companies" and that Russian operatives were able to penetrate the voter registration databases and access voter registration data from Illinois and at least one other state. (*Id.* at 8, 22.)

Counties in Georgia were targeted as well. In July 2018, Special Counsel Robert Mueller released an indictment that alleges that a Russian operative "visited the websites of certain counties in Georgia, Florida, and Iowa" on or about October 28, 2016. (Doc. 471-7 at 3.) As a result, the SSCI report recommends that state officials "[u]pdate software in voter registration systems" and "[c]reate backups, including paper copies, of state voter registration databases." (SSCI Report at 57.)

D. The State's expert Dr. Shamos essentially agrees that Georgia's DRE/GEMS system is not reliably secure.

One might recall that Defendants surprisingly presented no witness with actual computer science engineering and forensic expertise at the 2018 preliminary injunction hearing to address the impact of the breach of the Center for Election Systems servers housed at Kennesaw State University, or the specifics of any forensic evaluation of the servers, DREs, or the State and County processes for data transfer using removable media connected to public facing computers and the private GEMS servers. Now in response to the Plaintiffs' renewed request for injunctive relief in time for the Fall 2019 election cycle, the State Defendants offer testimony from two cyber-security experts who had been retained by the State in 2017: Theresa Payton of Fortalice Solutions, whose findings and testimony are addressed later, and Dr. Michael Shamos.

***19** The State offers Dr. Shamos to rebut and discredit the testimony of Plaintiffs' experts Dr. Alex Halderman and Dr. Richard DeMillo regarding the security vulnerabilities of Georgia's DRE voting machines and election system management infrastructure. Dr. Shamos was not asked to address the questions of ballot secrecy, post-election audits, electronic pollbook corrections, or voting system security evaluation and remediation.

Dr. Shamos holds strong opinions regarding the vulnerabilities in paper-ballot voting systems when compared to what he describes in his declaration as the "supposed" risks and vulnerabilities of DREs identified by Plaintiffs and their experts. (*See* Shamos Decl. ¶¶ 33, 35.) As explained below, however, Dr. Shamos appears to be an outlier to the rest of the scientific community. According to Dr. Shamos's declaration offered in conjunction with the State's opposition brief, a paper ballot based voting system "is demonstrably less safe," than the DREs currently used by the State of Georgia. The central underpinnings of Dr. Shamos's criticisms of Plaintiffs' request for a switch from DREs to hand-marked ballots in his declaration are:

(i) Voters cannot be trusted to properly mark ballots by hand so that they will be interpreted as constituting a vote as the voter intended and therefore accurately counted by election officials, (Shamos Decl. ¶¶ 36, 38, 46-52);

(ii) There is abundant evidence of fraud and tampering with paper ballots throughout the nation's history, (*id.* ¶¶ 36, 39-46);

(iii) There has never been a verified incident of tampering with an electronic voting machine being used in an election (*id.* ¶¶ 33-34, 115);

(iv) No expert has offered a feasible scenario for such tampering under actual election conditions, (*id.* ¶¶ 64-68, 69-73, 76, 84, 89, 91, 118); and

(v) If attempts to tamper with voting machines had been made, they would be detectable, (*id.* ¶¶ 74, 76, 77, 92, 93, 97-98, 103, 115, 117, 122, 132, 133).

According to Dr. Shamos in his July 10, 2019 declaration, "the issue is not whether a system is vulnerable in isolation, but whether it is vulnerable in actual use, considering that representatives of the political parties are watching with sharp eyes, and the administrators of elections (who are also being watched) are interested in clean elections." (*Id.* ¶ 67.) Nine days later, however, during his videotaped deposition, Dr. Shamos walked back much of what he'd previously stated in his declaration and admitted that Georgia's current election system had significant security gaps and weaknesses that cast serious doubt on the viability of its continued use in future elections if left unremediated. Thus, the totality of evidence in this case reveals that the Secretary of State's efforts in monitoring the security of its voting systems have been lax at best – a clear indication that Georgia's computerized election system is vulnerable in actual use.

In his declaration Dr. Shamos, lays out a laundry list of drawbacks to paper ballots that in his opinion make them less safe than DREs. These include: a paper ballot is the sole record of the voter's choice that, if lost, cannot be recovered; [35] anytime another human touches a paper ballot, it can be modified; [36] hand-marked paper ballots can be subject to an overvote simply by "holding a pencil lead under one's thumbnail," causing the loss of a legitimate vote; and ballot boxes can be lost or stolen on their way to the tabulation center. (Shamos Decl. ¶¶ 36, 39.) In his subsequent deposition, Dr. Shamos clarified that it is not his opinion that paper ballots should not be used, but that one should understand the risks of them: "using paper ballots is a rational means of voting. It has risks and vulnerabilities just like DREs. They are different, but they are risks." (Shamos Dep. at 42, 44; *see also* Dep. at 123 ("I think voters should have their eyes open as to what the real risks are, and there are real risks in paper systems; there are real risks in DREs systems, too.").) In an article authored on December 3, 2008, entitled "Voting as an Engineering Problem," Dr. Shamos wrote, "Voting machines are among the least reliable devices on this planet. It has been reported anecdotally that approximately 10 percent of DRE machines fail in some respect during the average 13 hours they are in use on election day. In some cases, the percentage is much higher (Bishop et al., 2005)." *Available at* https://www.nae.edu/7671/VotingasanEngineeringProblem.

***20** According to Dr. Shamos, one pitfall with paper ballots is the use of optical scanners to tabulate votes. Dr. Shamos states in his declaration that optical scanners that use infrared light to read ballots may not accurately read certain paper ballots. [37] (Shamos Decl. ¶ 55.) First, he posits that ballots may be printed that look blank but have already been pre-voted by using white ink to fill in the voting ovals. In that scenario, "any race in which the voter votes for the preselected candidate will count (because the voter made a mark over the prevoted position), while any other selection will result in an overvote." (*Id.*) To Plaintiffs' point that paper ballots serve as a verifiable backup record to the electronic record captured by the scanner, Dr. Shamos admits that manipulation of an optical scan ballot system could be discovered and negated by a manual/hand re-count using the paper ballot itself as a verification of the voter's intent. [38] (*Id.* ¶¶ 55, 57.)

Second, Dr. Shamos suggests that the sensitivity of each optical scan sensor can be adjusted manually inside the machine in order to manipulate how the scanner will scan and tabulate votes from certain ballots. (*Id.* ¶ 56.) For example, if one desires to suppress votes in a precinct known to favor a particular political party, the sensitivity of the sensor may be set very low to only recognize extremely dark marks as votes, or set very high to pick up variations in paper reflectivity as votes causing a large number of overvoted ballots. (*Id.*) Again, he acknowledges that the correct choices can be counted through either a hand re-count or if the ballots are re-counted on a different scanner. [39] (*Id.*) Dr. Shamos does not indicate whether there are any documented instances of these forms of tampering with optical scan ballots and scanners. Nor has he undertaken any analysis of the reliability of Georgia's current processes or procedures for handling absentee and provisional paper ballots. (Shamos Dep. at 48.)

In his deposition, Dr. Shamos explained that modern optical scanners that produce images of ballots, when used at the precinct level, are safer and more reliable than older infrared technology. [40] (*Id.* at 26-27.) These precinct count systems produce vote totals and ballot images that can be compared with the actual ballots for post-election verification. (*Id.*)

***21** In his declaration, Dr. Shamos also criticizes Dr. Halderman and Dr. DeMillo's testimony regarding the susceptibility of DREs to malicious interference as conjecture. Dr. Shamos states that Russia has no capability of interfering with Georgia elections "except through the Internet, and neither GEMS nor Georgia's DREs are accessible through the Internet." (Shamos Decl. ¶ 64.) In his deposition, however, Dr. Shamos acknowledges several potential penetration points for contamination. (*See* Shamos Dep. at 114 (testifying that penetration points for polymorphic viruses and back door intrusions could include insiders and could occur if the election tabulation system/GEMS server was not air gapped).) Dr. Shamos agreed that a political operative could bribe an insider to tamper with the DREs or swap out a memory card infected with malware that is used to program the voting machines on election day – and that would be a "realistic penetration factor" with Georgia's current election system. (Shamos Dep. at 50, 82.) For example, "[t]he system that the memory card gets – gets put into gets infected ... it's conceivable that any other memory card you put in that system, the malware would also copy itself to that memory card, and so there could be a kind of biological distribution mechanism like that." (*Id.* at 83; *see also* Shamos Decl. ¶ 77 (acknowledging the potential for Dr. Halderman's scenario of the propagation of vote-stealing malware via removable memory cards to a large population of machines).) Dr. Shamos further testified that assuming that the malware could exploit a vulnerability in the interface between the DRE and the GEMS server that are connected by a local area network, the malware would potentially infect the GEMS server and be transmitted to other DRES that are also connected to this local network. (Shamos Dep. at 84; *see also* Dep. at 119 (testifying that if malware is on the memory cards it can be propagated between GEMS and the DREs).) According to Dr. Shamos, there would be detectable evidence of this "if one chooses to look, and it doesn't evade parallel testing." (*Id.; see also id.* at 88 ("Remember all of this stuff leaves evidence if one chooses to look.") In his declaration, Dr. Shamos opines that an infected memory card is easily detected because the contents of the infected card differ from those of legitimate memory cards. (Shamos Decl. ¶ 77.) Thus, he states it is important "to verify the integrity of a memory card before inserting into a machine. An authorized copy of the memory card for the election in each precinct can be maintained at the county and a hash value computed. The individual precincts, prior to installing the memory card, would plug it into a PC to compute its hash value, which would then be compared with the true value." (*Id.*) When asked whether there is any evidence that election workers in Georgia perform such tests on each memory card before opening the machines for voting, Dr. Shamos testified: "I don't know of any, I don't know that they do. I think they should ... I don't know of it being done. I seriously doubt that it was done." (Shamos Dep. at 102.)

In his declaration, Dr. Shamos acknowledges that DREs are computers that can be hacked if the hacker is given "unfettered access" to it. (Shamos Decl. ¶ 66.) Dr. Shamos goes further in contending that "the issue is not whether vulnerabilities exist, but whether there is any rational possibility of exploiting them in a system that involves tens of thousands of non-networked machines distributed among Georgia's 159 counties, all of which conduct elections independently," and that in order for every DRE to be vulnerable to cyberattacks the hacker must be given unlimited access to each machine. (*Id.* ¶¶ 70, 72.) Contrary to the statements in his declaration, Dr. Shamos admitted in his deposition that a hacker would not necessarily need access to thousands of DREs in hundreds of counties to infiltrate Georgia's election system. (Shamos Dep. at 85.) A hacker could affect a single memory card with malware that could possibly propagate to the local GEMS server and to other DREs. (*Id.*) Dr. Shamos also acknowledges that infecting only a relatively small number of DREs could affect the outcome of close elections. (*Id.* at 86.) Dr. Shamos has not examined Georgia's election systems to determine whether it is in fact possible. (*Id.*)

Once malware is installed, Dr. Shamos contends the malware is detectable because it differs from the legitimate software and "simply by dumping the contents of a machine's memory one could detect the difference during an audit." (*Id.* ¶ 72.) But he admits in his deposition that to his knowledge Georgia does not, and has never conducted, such audits of the software and memory on its DREs to detect the presence of malware. (Shamos Dep. at 114.) Dr. Shamos further admits that the printout generated by DREs of each ballot cast would not reveal whether any software had been tampered with. (*Id.* ¶ 63.) Again, Dr. Shamos is not aware of any evidence that the State of Georgia has undertaken any forensic examination of Georgia's DREs for contamination. (*Id.* at 88.) Nor has he seen any evidence or have any reason to believe that Georgia has performed any review of the computers used by the State or the counties on the GEMS network to determine if there is any infection of the election system because it would not be routine procedure. (*Id.* at 103.)

Dr. Shamos criticizes Dr. Halderman for educating the Court about the serious vulnerability in the AccuVote TSX DRE machine used in Georgia that was discovered in 2006 by Harri Hursti [41] because he assumed the vulnerability existing in Georgia "was remediated a long time ago" – which was not so. (*See id.* ¶ 75.) As discussed above, based on his review of the AccuVote TSX source code and after conducting tests on the system in 2006, Hursti found numerous vulnerabilities with the AccuVote TSX, the most serious of which is that the operating system software in the machines enables "a malicious person to compromise the equipment even years before actually using the exploit, possibly leaving the voting terminal incurably compromised." Harri Hursti, *Diebold TSX Evaluation, Security Alert: May 11, 2006, Critical Security Issues with Diebold TSX*, Executive Summary at 2. Hursti further noted, "[i]t is important to understand that these attacks are permanent in nature, surviving through the election cycles. Therefore, the contamination can happen at any point of the device's life cycle and remain active and undetected from the point of contamination on through multiple election cycles and even software upgrade cycles." *Id.* at 4. The software defects "compromise the underlying platform and therefore cast a serious question over the integrity of the vote. These exploits can be used to affect the trustworthiness of the system or to selectively disenfranchise groups of voters through denial of service." *Id.* at 2. In his deposition, Dr. Shamos characterized the vulnerability found by Hursti in 2006 as "one of the most severe security flaws ever discovered in a voting system," up to that time. (Shamos Dep. at 115.) And he acknowledges that there are more serious flaws that have been discovered with DREs since that time. (*Id.*)

***22** Following Hursti's 2006 security alert, Diebold was forced to upgrade and create a security patch for the vulnerable TSX software. While Dr. Shamos [42] insisted that the Pennsylvania Secretary of State threaten Diebold with decertification unless the vulnerability was remediated before the next election, he has no direct knowledge that Georgia availed itself of the security patch on its DREs that run on a software version from 2005. (Shamos Decl. ¶ 75; Shamos Dep. 116-17.) Dr. Shamos admitted that he is unaware of any evidence that Georgia has in fact implemented the patch and that "it should be done before the machines are used again." (Shamos Dep. at 117.)]

Dr. Shamos has "never [been] a Diebold fan," and believes "the voting machine manufacturers did not pay what [he] thought would be sufficient attention to security, secrecy and various other issues. They were interested in selling machines." (*Id.* at 118.) In a Washington Post article published in 2006, Dr. Shamos is quoted as saying, "What are these companies really doing? They don't seem to have embraced the seriousness with which people in this country take their elections. It's been kind of an adversarial thing where companies want to make profits and they just haven't spent enough time and energy designing secure

systems." (*Id.*) When asked by Plaintiffs' counsel in this case at his July 2019 deposition whether it was his view that the machines are better now, Dr. Shamos testified that "if the machines are in the state that they were in 2006, no." (*Id.*)

Dr. Shamos states in his declaration that he "was the inventor of parallel testing in 2004," that can detect the presence of malware on electronic voting machines. (Shamos Decl. ¶ 97.) According to his declaration, "in proper parallel testing, officials select a precinct at random and designate a machine to be voted, but its votes will not be counted in the election. The officials then cast a predetermined set of ballots (generated at random based on the political demographic of the precinct) while the election is in progress. If malware is present that alters votes, the reported totals will not correspond to the predetermined ones, and the machine will be revealed as having been altered." (*Id.* ¶ 98.) Dr. Shamos "does not deny" that malware can be created that would "be able to detect it was under test and would operate properly but later sense that it was actually being used in an election and would manipulate votes, then erase itself at the close of the election." (*Id.* ¶¶ 97, 99.) However, in his opinion as stated in his declaration "parallel testing ensures that it would be discovered." (*Id.* ¶¶ 97; 132.)

But in his deposition, Dr. Shamos clarified that the description of parallel testing provided in his declaration was incorrect. Instead, he explained that parallel testing should not be limited to a single precinct, but instead should be conducted on voting machines in each county conducting an election, and in larger counties you would conduct testing in multiple precincts. (Shamos Dep. at 105.) The correct number of voting machines and precincts needed for parallel testing is determined on a statistical basis. (*Id.*)

Dr. Shamos further testified that he is aware that the Georgia Secretary of State's office conducts parallel testing on a single DRE out of the 27,000 used in the state and that he "castigates Georgia for not following [his] recommendations on how parallel testing should be done." (Shamos Dep. at 105-106.) Dr. Shamos has no confidence "in a procedure which selects one machine out of 27,000." (*Id.* at 107.) "The only thing that parallel testing on a single DRE will reveal is whether all of the voting machines in the state have been infected, because then the machine being tested would also have been infected." (*Id.*)

***23** In addition to parallel testing, Dr. Shamos suggests that to determine the accuracy of voting machines during an election "it is possible to open machines for voting, then upload their software for comparison with the authorized software. If the comparison passes, then voters are allowed to use the machine. Otherwise, the machine is impounded." (*Id.* ¶ 101.) Dr. Shamos agrees with Dr. Halderman as to the futility of detecting post-election malware that has erased itself when the polls close. (*Id.* ¶ 103.) For this reason, Dr. Shamos suggests that a forensic investigation should be performed before or during the election as part of parallel testing. (*Id.*) In his deposition, however, Dr. Shamos admitted that he knew of no evidence indicating that Georgia reviews the integrity of the DRE software on its machines prior to putting them in use for voting – "other than the defective parallel testing" – and he doubts they do it. (Shamos Dep. at 108, 113.)

Dr. Shamos has no doubt that state actors are constantly trying to infiltrate public-facing servers in Georgia. (Shamos Decl. ¶ 114.) Dr. Shamos believes it could be determined whether advanced persistent threats have infiltrated Georgia's vote counting systems through a forensic examination of the code on those systems, though he acknowledges the State has undertaken no such review of its election systems. (*Id.* ¶¶ 114, 122; Shamos Depo. at 113-14.)

Dr. Shamos agrees with Plaintiffs' experts and the general scientific consensus that Russia's attacks on the voting process in the United States in 2016 were indeed unprecedented. (Shamos Decl. ¶ 61.) It is his opinion that if Russia's attempts to intrude into voter registration systems had been successful, all forms of voting – DRE, opscan, hand-counted paper – would be affected. (*Id.; see also* Shamos Dep. at 66 (testifying that because only registered voters are permitted to vote, any interference with voter registration databases affects all forms of voting because voters will show up to the polls and be told they do not get to vote).) By removing a voter from the registration rolls, the voter is prevented from voting, except by provisional ballot. (*Id.*) Dr. Shamos believes that all provisional ballots cast by voters whose registration information had been manipulated would "eventually be counted." (*Id.*) This mistakenly presumes: (1) all such voters were offered a provisional ballot; (2) all such voters were given instructions on how to cure their registration status in the 3-day period allowed under Georgia law prior to election certification by the Secretary of State; (3) that the registration status (occurring as result of error in the State's database) could be cured; and

(4) that the counties employ proper procedures for processing and counting provisional ballots. As this Court is aware based on its handling of this case and a recognition of the legal issues addressed in other 2018 Georgia election cases filed in the Northern District of Georgia, these presumptions by Dr. Shamos are not all correct.

In his deposition, Dr. Shamos acknowledges that an intrusion could be made into the voter registration systems to target particular voters based on voter demographics. (*Id.* at 67.) For example, Dr. Shamos agreed that in a state like Georgia where voters in a metropolitan county overwhelmingly lean democratic as opposed to the more rural counties that tend to vote republican, one could attempt to manipulate the election results by disenfranchising particular voters by removing them from the registration of a particular county. (*Id.* 67-68.) In his opinion, interference with the voter rolls would result in a complete loss of faith in the entire voting process. (*Id.* at 66.)

Dr. Shamos explained what it means for a computer system to be air gapped:

> I have different components of a system, I have some in this room and I have some in that room. If it is not possible for one computer to communicate with another computer except by the physical moving of media from one to other, they are air-gapped. It doesn't directly relate to the Internet. But, of course, if I can get to your system through the Internet, it's not air gapped.

***24** (Shamos Dep. at 70.) A system where removable media is sometimes connected to an Internet-facing computer and then also connected to that standalone system is not considered air gapped. (*Id.*) Computer systems used "for election management should never, at any point in their life, have ever been -- ever be connected to the Internet," including "by removable [ ] media that at some point was connected to an Internet-facing computer ... because of the possibility of infections from malware." (*Id.* at 70-71.) The same is true of a server that is connected to phone lines by a modem: "air gapped refers to a gap between two things. So if it's connectable by a phone line to something else, it's not air gapped from that thing." (*Id.* at 71.) Jurisdictions that transmit vote totals via modem to a central count station are not air gapped and are not secure:

> Q. And you're aware of instances involving infiltration in computer systems using phone lines historically, right?
>
> A. Yes. I'm not a phone line fan when it comes to voting systems.
>
> Q. Because they can be infiltrated.
>
> A. Because they can be, and you don't know whether they have been, and you just don't know what's going on.

(*Id.* 71-72.)

Dr. Shamos was told by counsel for State Defendants that Georgia's tabulation system – i.e. the GEMS servers and databases – were not Internet facing and he assumed that information to be accurate in offering the opinions in his declaration. (Shamos Dep. at 73.) He also reviewed "documentation years ago" regarding the GEMS architecture that indicated the GEMS servers are air gapped and are not Internet-facing, but he "can't swear that at no point in its life have any of the GEMS servers not been connected to the Internet." (*Id.* at 74, 77-78.) Dr. Shamos has not personally confirmed that the Georgia GEMS servers and databases are not accessible through the Internet and testified that "[i]t would be very difficult for me to do that, because as soon as I left a GEMS system, they could plug it into the Internet. Even though it wasn't connected when I looked at it, it could be connected five minutes later." (*Id.* at 80.) Except for his trip to Atlanta on July 19, 2019 for his videotaped deposition in this case, Dr. Shamos has not been in Georgia for twenty years.

In sum, in Dr. Shamos's view, voters cannot have absolute confidence in any voting system, including DREs, because all voting systems have risks and vulnerabilities. (Shamos Dep. at 46.) Dr. Shamos, however, is an outlier in his views about the legitimacy

of continuing to use DREs in the face of a mountain of identified critical security flaws and risks and in his attitude about the potential for the hacking of DREs and election management systems in the context of actual elections.

In a declaration offered in support of Plaintiffs' motions here, Dr. Andrew Appel, an appointed member of the National Academies of Science, Engineering and Medicine (NASEM) Consensus Study Committee on the Future of Voting, explains that Dr. Shamos's claims that DREs are more reliable than voter verified paper ballots in his July 10, 2019 Declaration go against the weight of scientific consensus. (Appel Decl. ¶¶ 30-38, Doc. 510-2; 524-2.) In his fifteen years of studying voting machines from 2004 to 2019, Dr. Appel attests that he has spoken and corresponded with, and read the work of well over 100 experts on the computer science and security aspects of voting machines. (*Id.* ¶ 38.) He has reviewed the scientific literature since 2007 on voting machines with publications by dozens of scientists. (*Id.*) On this basis, Dr. Appel understands that, "with one exception, all computer-science experts on voting machines recognize that voting machines are not difficult to reprogram (to "hack" if reprogrammed without authorization) and therefore it is unacceptably insecure to use paperless DRE voting machines in public elections." (*Id.*) "The sole exception," Dr. Appel has identified across his extensive experience and research in the field is Dr. Michael Shamos. (*Id.*)

***25** The NAS Committee on which Dr. Appel served extensively studied the vulnerabilities of electronic voting systems in use in the United States, and had no difficulty in reaching consensus that "[e]very effort should be made to use human-readable paper ballots in the 2018" and that "[a]ll local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election." [43] (*Id.* ¶¶ 31-35) (quoting the NAS's September 2018 Report). According to the NAS report, cybersecurity experts generally agree that cybersecurity risks are inherent when states rely entirely on computers for voters to cast ballots and was particularly concerned about the risk of undetectable cyberattacks on DREs that lack a "paper artifact that could be manually counted." (Doc. 285-1, Ex. 1 at 77-78.) NAS reports are "subjected to rigorous peer reviews before they are released to the public," and "a consensus report of the NAS ... represents the highest authority that the U.S. Government can rely upon when it seeks to be advised on matters of science, technology and engineering." (DeMillo Decl., Doc. 285-1 ¶ 8, 9.)

As discussed above, contrary to Dr. Shamos's singular voice, the U.S. Senate Select Committee on Intelligence concluded that "[p]aper ballots and optical scanners are the least vulnerable to cyberattack." (SSCI Report at 59.) Dr. Appel further explains,

> Contrary to Dr. Shamos's conclusions, Dr. Halderman's description of how DREs can be easily hacked is consistent with the scientific consensus, as described in peer-reviewed academic publications and in other venues, and agrees with my own research and study of this issue. Dr. Shamos's claims (of the supposed difficulty in hacking) in his [declaration] are incorrect, unsupported by scientific research, contradicted by the published scientific research, and inconsistent with the scientific consensus.

(Appel Decl. ¶ 20, Doc. 510-2; 524-2; *see also* ¶¶ 21-24 (detailing a variety of documented and tested ways in which a DRE can be "hacked" and an election management system "hijacked"); ¶ 26 (noting documented cases of intrusions by stealthy hackers that survived years without detection). Therefore, according to Dr. Appel, "Dr. Shamos is incorrect in asserting that it would be impractical to hack Georgia's DREs by a fully remote attack, and that any such attack would be readily detected." (*Id.* ¶ 27.) Dr. Shamos appears to be a lone wolf in his belief that DREs are acceptably insecure and is therefore "an outlier to the scientific community." (Appel Decl. ¶ 38, Doc. 510-2; 524-2.)

But even Dr. Shamos has no confidence in Georgia's use of DREs that run on outdated and unsecure software from 2005 or in Georgia's use of deficient parallel testing [44] as a means for verifying the accuracy of its outdated DREs. (*Id.* at 107, 117.) While Dr. Shamos offered all sorts of opinions in his declaration to support Defendants' opposition to a request for relief requiring them to abandon DREs for 2019 elections, his testimony presented by video deposition at the injunction hearing in many ways provides further expert evidence in support of Plaintiffs' position, as well as the expert testimony of Dr. Halderman and Dr.

DeMillo. Rather than defeating Plaintiffs' evidence, Dr. Shamos's testimony reaffirmed the credibility of Plaintiffs' experts' concerns (as substantiated by the national consensus) of the significant security risks in Georgia's current electronic voting system. This is especially true considering the State Defendants' attack of Dr. Halderman's testimony that Georgia's GEMS servers and databases are not air gapped and are not isolated from cyber intrusion as the State's elections and information technology representatives believe. (*See also* Appel Decl. ¶¶ 24, Doc. 510-2; 524-2) ("Election-management computers must be routinely (directly or indirectly) connected to the internet (or to the phone system, which nowadays is the same thing) for a variety of purposes, including the dissemination of election results. It is widely known (and documented) as a matter of science ... that computer systems connected (directly or indirectly) to the internet are often hacked, that is, infiltrated by malicious hackers."). As evidenced by Michael Barnes's testimony in both the 2018 and 2019 injunction hearings regarding the use of phone and modem lines by counties, his own use of USB drives plugged back and forth between the private GEMS server and his public facing computer, and the State's reliance on ballot building contractors working independently in their homes without direct security oversight – Georgia's election system is not in fact an impenetrable secure air gapped system safe from intrusion or an advanced persistent threat.

E. "What's Past is Prologue." [45]

***26** From approximately 2002 through at least December 2017, the Secretary of State contracted with Kennesaw State University's Center for Elections System through the Board of Regents of the University of Georgia to provide all the nuts and bolts management of the GEMS and Georgia's election system. [46] CES maintained the central election server, for Georgia's GEMS system; managed the State's GEMS server; stored and managed GEMS State and County election and voter data; furnished data to create the lists of voters for electronic express pollbooks used in elections in every precinct across the State; performed all ballot building processes required for the County elections offices' issuance of the specific election ballots at the precinct level; provided support for all jurisdictions in the election process and in support of DREs, and overall played an essential role in the operation of elections. (Doc. 258-1.) In effect, the Secretary of State's Office contracted out its election management operational responsibilities to CES until the public exposure of major data management security lapses in March 2017 catalyzed the Secretary of State's Office's termination of the CES's services at KSU, effective January 1, 2018.

Merle King, served as Executive Director throughout the Center's existence, and Michael Barnes served on the Center's staff starting in 2005 and as its Director from 2010 during the years leading up to the CES's closure and his subsequent transfer in January 2018. Barnes immediately became Director of the CES at the Secretary of State's office. [47] No other CES staff transferred to the SOS office. In other words, when the Court held its first preliminary injunction hearing in September 2018, the SOS's office had assumed the functions of the CES at KSU ("CES/KSU"), less than a year earlier, on January 1, 2018. (Doc. 472-4 at 2.)

The State Defendants effectively dismiss the significance of the CES/KSU data breach, data systems mismanagement, and record destruction. But as the Court assesses the current operation of Georgia's voting systems and voter registration databases, the legacy of these events stands out.

The Court's September 17, 2018 Order summarized these events as follows:

> In August 2016, Logan Lamb, a professional cybersecurity expert in Georgia, went to CES's public website and discovered that he was able to access key election system files, including multiple gigabytes of data and thousands of files with private elector information. The information included electors' driver's license numbers, birth dates, full home addresses, the last four digits of their Social Security numbers, and more. Mr. Lamb was also able to access, for at least 15 counties, the election management databases from the GEMS central tabulator used to create ballot definitions, program memory cards, and tally and store and report all votes. He also was able to access passwords for polling place supervisors to operate the DREs and make administrative corrections to the DREs. Immediately, Mr. Lamb alerted Merle King, the Executive Director overseeing CES, of the system's vulnerabilities. The State did not take any remedial action after Mr. King was alerted.

> In February 2017, a cybersecurity colleague of Mr. Lamb's, Chris Grayson, was able to repeat what Mr. Lamb had done earlier and access key election information. Mr. Lamb also found, around this time, that he could still access and download the information as he had before. On March 1, 2017, Mr. Grayson notified a colleague at Kennesaw State University about the system's vulnerabilities, and this led to notification of Mr. King again. Days later, the FBI was alerted and took possession of the CES server.
>
> ***27** The Secretary of State has since shut down the CES and moved the central server internally within the Secretary's office. But on July 7, 2017, four days after this lawsuit was originally filed in Fulton Superior Court, all data on the hard drives of the University's "elections.kennesaw.edu" server was destroyed. And on August 9, 2017, less than a day after this action was removed to this Court, all data on the hard drives of a secondary server – which contained similar information to the "elections.kennesaw.edu" server – was also destroyed. As discussed more fully later in this Order, the State offered little more than a one-sentence response to these data system incursions and vulnerabilities at CES.

Curling, 334 F. Supp. 3rd at 1310. The Court further found after hearing Mr. Barnes's testimony at the September 2018 preliminary injunction hearing:

> Mr. Barnes professed effectively no knowledge about the ramifications for the state's voter system or remedial measures in connection with Mr. Lamb's accessing the CES's voter registration databases – which was filled with millions of voter records with personally identifiable information, passwords for election day supervisors, and the software used to create ballot definitions, [DRE] memory cards, and vote tabulations.

Id. at 1323.

The Court's closer examination of the record evidence now is even more disturbing. In a detailed email dated August 28, 2016, Mr. Lamb brought to Merle King's attention the CES server exposure and compromise, data exposure, software flaws and security issues – all of major magnitude – that rendered the CES-managed voting system highly vulnerable and subject to dysfunction, erroneous data outputs, manipulation and attack.[48] (*See generally* Doc. 258-1 at 125-255, 251-253.) Mr. King communicated with both Mr. Barnes and KSU Chief Information Officer, Stephen Gay, and others regarding Lamb's detailed email. And Barnes in turn emailed Mr. Gay about the "unsolicited email" from Mr. Lamb. (Doc. 258-1 at 249-250) Despite his prior role as CES/KSU Director and current CES Director at the SOS, Mr. Barnes could recall little or what expressly was done after the August 2016 communication except that CES "got rid of" the data and did not look at it or do any forensic review of the files Mr. Lamb was able to download.[49] (Doc. 472-10 at 56.) But the email communications up until mid-October 2016 between information technology staff, in fact, kept Mr. Barnes fully in the loop regarding the host of serious software threats, website holes, and data security exposures that they had now confirmed after receipt of Lamb's letter and that they were still struggling to address.[50] By the end of October, the record goes silent and nothing appears to have happened or been done until March, 2017.

***28** As Mr. Lamb never heard from Mr. King or other CES staff after his original August 28, 2016 email, his colleague, Chris Grayson, who had verified Lamb's previously flagged identification of the security risks contacted a KSU faculty member, Andy Green, a lecturer on Information Security and Assurance. Mr. Green similarly confirmed the significant voting directories' exposure and election officials' credentials exposure vulnerability, among other vulnerabilities. Green then directly contacted Stephen Gay via email to address this issue anew and in his intermediary capacity commented that in his view, the cybersecurity professional (Lamb) who had identified these significant issues and the organization he was affiliated with were acting in good faith and seemed to want to give KSU an opportunity to remedy these problems before contacting the media. Gay later that night wrote Merle King that his tech security response team had also recreated the directory vulnerability on elections.kennesaw.edu

earlier described. Gay relayed that his team had pulled "voter information in database files for counties across the state and data elements including the DOB, Drivers License Number, Party Affiliation, etc. Understanding the risk associated with this vulnerability, we have closed all firewall exceptions for elections.kennesaw.edu to contain the incident ...." (Doc. 258-1 at 226.)

An information security engineer in KSU's Information Security Office then on March 4, 2017 ran a special scan of the CES backup server and identified a number of other files open to all KSU users, the top one of which contained 5.7 million records with personal identifying information. (*Id.* at 201-202.) The Associate Executive Director for KSU Information Security therefore recommended that CES close down the server – and King directed Barnes to do so that day. Sometime in the ensuing week, with the pervasiveness of the data breach and vulnerabilities finally confronted, Mr. Gay contacted federal investigators who took temporary possession of the Elections server.

A detailed incident report, dated April 18, 2017, generated by the KSU Information Technology Information Security Office identified the seriousness and extensiveness of ten security issues posed by the CES information technology systems and data breach, with the top three identified as follows:

1. **Issue:** Poor understanding of risk posed by the Center for Election Systems IT systems. While a previous server scan and an external researcher had helped UITS understand the high threat level of CES systems, the lack of understanding the hosted data set led to an incomplete picture of the asset value. This resulted in the existence of a high risk server (High Asset Value / High Threat Level) which should have been prioritized...

2. **Issue:** Elections webserver and Unicoi backsup server are running a vulnerable version of Drupal and vulnerable to exploitation.

Action Items: Elections (externally-facing) was seized immediately and Unicoi (isolated network) was seized thereafter

....

3. **Issue:** CES confidential data handling processes were not defined ...

(Doc. 1-2 at 99-102.) In other words, critical security issues that Lamb had identified in August 2016 finally caused major alarm bells to go off in 2017 when the University's Information Security Office investigated, independent of CES, following faculty member Andrew Green's communication. But in reality, CES had been advised of these *confirmed* critical vulnerabilities in October 2016 when the KSU Information Security Office had scanned CES's backup Unicoi server and when CES's own staff acknowledged they were merely juggling – but apparently no follow-up had occurred. (*See infra.*)

In late March 2017, KSU began arranging with SOS for the uploading of the CES/KSU Express Poll election files to the SOS server, with some transfer security protocols in place. There is no indication than any measures were taken to address the integrity of the database being transferred given the circumstances.[51] (*Id.* at 191-197.) The accessible files could have been and likely were open to access for far longer than the window of time between Lamb's original review in August 2017 and his second review in March 2017. In his declaration, Mr. Lamb articulated his view as a cybersecurity engineer that "[a]ny malware that may have been introduced during periods of security failure would very likely still be present on ExpressPoll books or on other voting system components which remain in use across the state." (Doc. 258-1 at 133.) This view as to the danger of contamination was similarly articulated by other cybersecurity experts in this case, including the State's expert and consultant, Ms. Theresa Payton.

***29** The Court well understands the challenges every state faces in running elections in this era. But the State Defendants' insistence that nothing amiss happened in the gaping breach and exposure of the CES/KSU electronic election management system and voter databases contradicts the evidence. Similarly, Defendants' blithe blindness to the potential reverberations that would follow the GEMS system and voter registration databases upon transfer to the SOS, after such an exposure and system management, contradicts the fulsome expert opinion and evidence provided in this case.

CES's executive staff were in the loop in all communications regarding the servers supporting the CES's operations, transfer of the election and data systems to the SOS, Open Records Act requests, and requisite records retention. And they were engaged as well when KSU retrieved and wiped the servers in the months after the FBI made forensic images of the servers.

Given the entire course of events described here, the Defendants' contention that the servers were simply "repurposed" and not intentionally destroyed or wiped is flatly not credible. [52] (State Defs.' Resp., Doc. 558 at 2, 11 - 14.) This is especially so given the sensitivity of these circumstances, state record retention requirements, and the correlation of the server destruction or erasures with the filing of litigation and removal of the case to the federal court. [53] Simply put, without reaching the issue of spoliation and presumptions or consequences, the Court seriously views the evidentiary import of the Defendants' handling of the servers and its connection to assessing other record evidence – and this course of conduct casts a disturbing shadow on Defendants' posture here. [54]

***30** Similarly, Defendants' denial and dodging before the Court regarding the known veracity of Logan Lamb's proactive alerts to CES/KSU as to the broadscale vulnerability of its election servers, software, and databases both undermines the credibility of Defendants' representations and signals the election system problems that would continue upon CES's transfer to the Secretary of State's Office. The scenario underlying the transfer of the CES's functions back to the Secretary of State's Office provides a troubling background context for the elections of 2018 and beyond. The Court recognizes, still, that some progress has been made – and that the State Legislature has moved forward in enacting new voting legislation to be implemented hopefully in future election cycles, *i.e.*, "as soon as possible." O.C.G.A. § 21-2-300. But in assessing the merits of the Plaintiffs' preliminary injunction motions and equitable relief issues, the Court is dealing with the here and now, and that bears the ongoing stamp of infection from the past and the serious problems of the current actual voting system in place.

The State Defendants argue that the Secretary of State's Office has made significant progress in assuring the security of the Georgia GEMS/AccuVote DRE election system and the digitized statewide voter registration system encompassed within the eNet software application. [55] The State purchased new computers for running the GEMS system after its transfer from KSU. And they contend they have addressed any alleged underlying structural election data system vulnerabilities, while at the same time minimizing such. In this connection, the State primarily relies on the testimony of its Chief Information Officer, Merritt Beaver, the Center for Election Systems (CES) Director Michael Barnes, and the SOS's retention of the Fortalice Solutions Company ("Fortalice") for consulting and assessment services.

Fortalice operates under the leadership of its CEO, Theresa Payton, who testified as a cybersecurity expert in Court and gave prior Declarations on behalf of the SOS. Fortalice was retained to conduct three cybersecurity evaluative assessments, [56] starting in the latter half of 2017. Two of its evaluations were performed before the September 2018 preliminary injunction hearing. The last general risk assessment report was performed from September 17, 2018 to November 30, 2018, and concluded two months after the Court's first preliminary injunction order of September 17, 2018. The evidentiary record is scant regarding what targeted remedial measures the State Defendants took after the last November 2018 report that relate to the election and voter registration systems at issue in this case as well as the record of voter harm caused by the administration of such systems. [57] But as discussed later, the Court certainly recognizes that the Georgia legislature enacted new legislation that provides major funding for implementation of a new electronic statewide voting system and other associated measures.

***31** The Court does not minimize the value of Fortalice's three reports and associated advice to the SOS as a positive step for the agency as a whole – or the value of the initial measures the SOS has taken to protect the perimeters of its agency electronic network security and move the system forward. But the core reality is that the State retained neither Ms. Payton nor its other expert, Dr. Michael Shamos, to conduct an actual cybersecurity review and analysis of the GEMS/DRE system and databases or the statewide voter registration system o Elections Division, apart from Fortalice's general risk assessment analysis.

Thus, the State's evidence presented in this case dodges the central issue posed by Plaintiffs' challenge to the DRE/GEMS system and eNet voter registration system: In light of well-established evidence of the vulnerability, security flaws, and the out-

of-date age of these systems and their software as well as national security and voting reliability concerns posed by continued use of a DRE/GEMS system – all that have been consistently recognized by major national studies and commissions of the highest rank – should the State be permitted to continue forward into another election cycle (and potentially beyond that cycle) with this system, particularly where Georgia's DRE system is incapable of producing a verifiable voter audit trail? And how should the Court address significant evidence of the unreliability of the eNet voter registration database and deficiencies in the eNet software that carry future consequences, even if management and housing of the database has been transferred to the State Elections Division as of July 1, 2019, while its vendor (PCC) maintains ownership and control over the software application? [58]

The Court is intimately familiar with the extensive record in this case. It views the overall evidence and national consensus authority and expert studies as favoring Plaintiffs' position. While taking all of this evidence into consideration as well as Georgia's new voting legislation to be implemented in 2020, the Court has also reviewed the SOS's evidence concerning its own progress to assess whether any form of injunctive relief is warranted to address the Plaintiffs' claims.

The Court has carefully reviewed Fortalice's risk assessment reports and the Secretary of State's associated change efforts and staff testimony. While the SOS's use of Fortalice's assessments is a constructive change tool, the evidence also demonstrates the steepness of the voting systems management climb before the SOS in the election cycles ahead. Moreover, the assessments provide a distinctly incomplete picture that fails to touch central issues in this case. The Fortalice assessment reports provide no testing and analysis of Georgia's GEMS/DRE voting system and software. They don't discuss the consensus in national expert opinion regarding the dangers posed by DRE-based unaudited voting systems, or any other issues related to operation of the GEMS system within the State and counties, the DRE machines, or the capacity for malware to be spread via the memory cards, data systems, and hugely dated software that support the system. While Fortalice partially evaluated PCC's eNet voter registration and express pollbook database and operations, it was not allowed to conduct penetration testing or to conduct a full evaluation of the dated software because of the SOS/PCC contract limitations. And even then, its assessment of the eNet voter registration systems and database rang serious alarm bells.

***32** The testimony of Theresa Payton and the restricted scope of the three cybersecurity evaluations performed makes clear that the surface of SOS cybersecurity issues was barely scratched. Most significantly, the SOS never asked or contracted with Fortalice to perform a specific cybersecurity evaluation of the security issues facing the SOS elections division and related county election offices, or the security vulnerability and integrity of the GEMS System both within SOS and its county elections counterparts, or the State's voting databases and electronic pollbooks. Ms. Payton forthrightly acknowledged in her hearing testimony that her organization focused solely on the perimeter "outskirts of the kingdom" of the Secretary of State's Office as opposed to a "specific vault" within the castle, such as the elections division and its operations. (Tr. Vol. 1, Doc. 570 at 287.) It was outside Fortalice's contract scope to focus on particular Election Division or GEMS data systems or conduct a review of the voter registration system software and operation, or the state election data systems' interface with SOS servers and SOS and County data systems and the cybersecurity and vulnerability issues posed by this interface. (*Id.*) Fortalice did not analyze that interface, nor did it attempt to conduct a "red team" directed penetration of the operations of the Center for Elections Systems within the SOS or in connection with the 159 counties, the GEMS database and software, or the eNet voter registration data system and pollbook software. (*Id.* at 286-288.) But all of these issues should have been squarely on Defendants' radar – and vividly so after the Court's order of September 17, 2018 and the ensuing 2018 election.

The first of the three Fortalice reports dated October 2017 identified 22 cyber security risks to the SOS, [59] with the ten leading ones identified as highest priority for remediation action, including risks associated with password management and security, access control, data security, and network and vulnerability management. [60] (PX 1, Doc. 561-1 at 5.) Significantly, Fortalice's Cloudburst team conducted penetration testing of the overall "outskirt" walls of the SOS network in July through August 2017 and was able to penetrate the SOS network "castle" walls and move around "fairly freely" within the agency's network and accounts. (Tr. Vol. 1 at Doc. 570, p. 288.) The Fortalice/Cloudburst team was able to compromise passwords and escalate its privileges to penetrate the SOS agency data system and access all local work stations and laptops and to establish footholds in a series of internal systems in SOS. (PX 1, Doc. 561-1 at 43-55.) Through this penetration, "emulating real-world attacker techniques," Fortalice's team gained control of domain administrator rights on the Georgia SOS connected network and in turn

obtained credentials to identify sensitive data, gained access to network security systems and the system enterprise architecture and system configurations within the SOS. [61] (PX 1, Doc. 561-1 at 42.) The October 2017 Fortalice Report identified these risks as high and concluded that it "recommends a heavy focus on prevention followed by investment in detection to actively manage threats that gain access to the network and keep them from resulting in a data breach or network compromise." (*Id.* at 39.)

Strangely, while SOS Chief Information Officer Beaver declared in his August 2018 and July 2019 affidavits in this case (Docs. 265-1, 472-2) that penetration testing had been conducted as an apparent indication of SOS remedial measures, his declarations never even hinted that Fortalice had actually successfully penetrated a major SOS network and data system that would allow the "attacker" access to information as to architecture of the entire system by obtaining control over the domain. [62] Nor did Mr. Beaver ever clarify, contrary to his representations in his 2018 affidavit, that the SOS had never requested or authorized focused penetration testing of the Election Division, the GEMS database and server system, the eNet or voter registration system, or the SOS election services vendors.

***33** Obviously, Ms. Payton, a national cybersecurity expert retained by the State, viewed the Fortalice penetration findings as impacting security and integrity of the entire SOS data system, including the election systems and data, because access to and interface between the public website and servers provides a host of routes into the system's architecture, administrative passwords, etc. And Dr. Halderman, Plaintiffs' expert, shared that view in his hearing testimony, which the Court finds is supported by the extensive expert evidence and authority Plaintiffs have provided. [63]

The October 2017 and February 2018 Fortalice Reports addressed the lack of security controls for Georgia's eNet voter registration data system and database. eNet is owned, operated, and maintained by PCC. On July 1, 2019 the SOS took over hosting eNet's voter registration database that creates the express pollbooks, but continued its contract with PCC for licensed use of the PCC software and for PCC's maintenance and support of the PCC application.

Fortalice's 2017 investigation revealed that a breadth of Georgia SOS personnel were able to log onto the election registration database without authentication mechanisms beyond a user name and password. Moreover, county election representatives (in 159 counties) could access the PCC database and distribute unlimited user accounts without oversight, and the software lacked "adequate controls to set role based security per accounts." (PX 1, Doc. 561-1 at 23.) The Report expressed an overarching concern about the lack of control and oversight the State maintained over the eNet voter registration system and database. (*Id.*) And this section of the 2017 Report concluded that:

> To determine the known vulnerabilities and risks to PCC as an entity and the eNet system, a thorough risk assessment of the organization and web assessment of the eNet system is recommended. Of additional concern, GA SOS lacks the right to audit the vendor's environment and/or obtain third-party assurance of controls on behalf of the GA SOS.

(*Id.*) But there is no indication in the record that this directive or testing was ever done, though in the Court's view, the PCC contract charges PCC with cybersecurity and accountability obligations that could be enforced.

The next assessment report Fortalice and Cloudburst performed was delivered to the SOS in February 2018 and focused exclusively on the voter registration database system operated by PCC. (PX 2, Doc. 561-2.) But Fortalice was not authorized to do penetration testing of PCC's operation. The Report described the old software in use as containing "known critical severity vulnerabilities." (*Id.* at 8.) The report concluded that "the most significant risk the Cloudburst Security team identified is the use of older, unsupported software to operate internet-facing web applications. The vendors for the software no longer provide updates to address known vulnerabilities." (*Id.* at 3, 13.) The #1 ranked risk in the Report involved PCC technologies and software because "these applications are externally-facing and have a wide use base and process important data, the

risk they pose is much higher." (*Id.*) The Report commented on the out of date vulnerable software that was subject to malware manipulation and attacks: "Malicious actors typically take advantage of known vulnerability of software or weak configurations. Cloudburst Security suggests robust vulnerability management and threat monitoring processes to increase the GA SOS environment's security." (*Id.*) The Report identified serious network construct issues as well in the PCC Georgia SOS environment. (*Id.* at 9.) And the PCC voter database system permitted "a list of IP addresses access to the internal systems bypassing the VPN" and "*does not block connections to the VPN from IP addresses of known threat sources or foreign countries*." (*Id.* at 11) (emphasis added). The February 2018 report also identified a chain of other related severe issues – including the transmission across the network of unencrypted database commands and content that "can be used to capture or modify communications between the internal servers leading to disclosure of sensitive data." (*Id.* at 18.)

***34** In total, the Cloudburst Security Team's October 2018 report identified 15 additional serious risks beyond the risks identified in the October 2017 Fortalice/Cloudburst report. Even without Cloudburst/Fortalice having been granted authority to conduct penetration testing, it documented an astonishingly grave array of deficits in PCC software for retention and management of the voter registration database as well as in the SOS and PCC's handling of the voter database.

Richard Barron, the Director for Registration and Elections in Fulton County, Georgia similarly identified a long-standing software defect in the Express Poll software dating back to 2006. "The 'Precinct Detail' in the Express Poll will display the information for the previous voter rather than the correct precinct for the voter standing before the poll worker. This results in the poll worker sending the voter to the incorrect precinct. If a voter in the wrong precinct goes to the precinct directed by the poll worker, the voter will find himself in another incorrect precinct and the 'Precinct Detail' tab will be no help again." (PX 16, Fulton county Board of Registration and Elections' Responses to Coalition Plaintiffs' First Interrogatories, Doc. 565-16 at 4.) [64]

The above findings coincide with and support the validity of the broad range of voter complaints in 2017 and 2018 regarding the inaccuracy and jumbled status of the voter registration records that burdened or deprived them of their voting rights, discussed later in this Order.

The SOS did not ask Fortalice to look again at the issues flagged regarding PCC's aged software, voter database and voting data security issues in the February 2018 report or to follow-up on whether PCC had implemented any of its recommendations. (Tr. Vol. 1, Doc. 580 at p. 40.) Indeed, in his testimony at the July 25, 2019 hearing, Mr. Beaver, the CIO of SOS, could not recall any of the identified issues or recommendations in the February 2018 report until he was furnished a copy of the report to review. The SOS – and its staff – have consistently previously maintained before this Court that there are no problems with the voter registration data system and database that generate the ExpressPoll electronic report that is the gateway for voters at the polls. Further, the SOS, which was in exclusive control of the Fortalice/Cloudburst Report information regarding the system's exposure of the voter registration database and its severe vulnerability at the time of the September 2018 preliminary injunction hearing, never disclosed any form of this information, even though the integrity of the voter database was squarely at issue then. (Testimony of Merritt Beaver, Tr. Vol. 1. at 65-67.) In this same vein, Defendants contended that Logan Lamb's ability to access through the KSU CES server multiple gigabytes of voter registration data from CES databases filled with the personal identifying information of millions of Georgia voters as well as county and state election staff passwords [65] was not of real significance. The evidence clearly indicates to the contrary.

***35** Fortalice's November 2018 assessment (its third and last report) returned again to focus on the "walls of the castle" of SOS as a whole. It found that SOS had fully remediated just three of the 22 deficits identified in October 2017. (PX 3, Doc. 561-3.) While noting the SOS's progress, Fortalice made twenty additional cybersecurity recommendations to protect the confidentiality, availability, and integrity of voting and voter data for the citizens of Georgia, fourteen of which were of low to no cost. And it identified the ten top cybersecurity risks from 2017 that carried over through 2018, three of which fell outside the scope of the 2018 assessment requested and were deemed unresolved. (The unresolved, out of scope, risks included: insufficient firewall protection for a SOS server; external website vulnerabilities; and "identity and access management controls and voter information privacy controls lacking on PCC's eNet system which houses Georgia's Voter Registration Database.") (*Id.* at 8-9.)

The Court will not delve into the details of the Fortalice system penetration efforts, because as Fortalice notes, the SOS limited the time frame allotted for external testing and an external hacker would not necessarily operate with such a time limit but would persist in attempts to obtain access. Fortalice therefore assumed the person or entity had breached the security wall and tested the scope of what the "attacker" could gain access to or control on the network if initial penetration was made. Once again, Fortalice was able through its probing to ultimately compromise accounts and gain access and control the domain administrator over the system. [66] "During the course of the assessment, Fortalice identified large repositories of voter registration information on network file shares accessible to all domain users" which pose security management challenges. (*Id.* at 29.) Its search of all network locations "was not exhaustive and additional review should be performed by SOS GA IT staff in order to identify all instances of sensitive data stored insecurely." (PX 3, Doc 561-2 at 19, 29.) At the July 25, 2019 hearing, Mr. Beaver affirmed that this related to PCC's management of the database and therefore that no more SOS follow-up would have been done. (Tr. Vol. 1., Doc. 570 at 69.) But this Fortalice finding was made in connection with SOS's storage of sensitive information hosted on file shares on its server(s) accessible to all domain users on the SOS system. (PX 3, Doc 561-2 at 19, 29.) In any event, Mr. Beaver testified that there were no updated reports conducted assessing this exposure of voter registration information on the SOS server or the integrity of the voter registration database after this November 2018 Fortalice recommendation. (Tr. Vol. 1, Doc. 570 at 69-71.)

The Court notes that on November 8, 2018 the Secretary of State filed Ms. Payton's declaration in another case before it relating to the functioning of the voter registration database. [67] *Common Cause Georgia v. Brian Kemp*, C.A. No. 1:18-cv-5102-AT (N.D. Ga. 2018) (Doc. 39). Payton's Declaration was filed in the period coinciding with Fortalice's Report in November 2018 and the November 2018 state elections. Ms. Payton declared that Fortalice had been retained to review an attempted infiltration of the SOS My Voter Page (MVP) website system. [68] Voters can use the MVP website to access their voter registration status, their mail-in application and ballot status, poll location, early voting locations, their elected officials, their registration information on file with the county office, a sample ballot for an upcoming election based on their specific residence, and the status of any provisional ballot they may have cast. They can also enter data on the MVP website to change their home address on the SOS voter registration records. [69]

***36** Ms. Payton's November 8, 2018 declaration indicated that Fortalice had seen multiple unsuccessful attempts to infiltrate the MVP system in its preliminary review of two weeks of logs, but that they had not yet seen any successful attempt in that initial review. Payton also represented that more work was underway to gather identifying information to determine the source of these infiltration attempts. No follow-up information was ever provided to the Court – and Mr. Beaver testified that no further reports beyond the November 2018 Fortalice Report were issued. At the hearing on July 25, 2019, Mr. Beaver dismissed the possibility that any hack onto the MVP could impact the voter registration data system then hosted on the eNet network because the MVP, though it contains voter registration information, only pulls voter data on a one-way basis from the voter registration data system. (Though the Court notes, anew, that voters – or someone acting in their stead – can input a changed address impacting their precinct designation via the website.) Payton's affidavit clearly did not suggest the view that an attack on MVP could not have collateral consequences for other portions of the voter registration or election system, even though she assumed MVP was hosted on a separate server.

Moreover, the Court wonders why the SOS would have engaged Ms. Payton to investigate this specific attack if there were no potential collateral consequences. Mr. Beaver's view neglects to consider that any cyber intruder's scraping of voter personal information from the My V0ter Page website could easily be used in other nefarious ways in the election process. Indeed, this concern clearly was identified in warnings provided by the FBI and the Department of Homeland Security as well as in the United States' 2018 indictment of multiple Russian agents.

Most recently, on July 1, 2019, the SOS assumed operational responsibility for hosting the SOS/PCC Technology database. However, the Secretary of State has continued to contract with PCC to maintain its software application for which needed patches are not available and which Fortalice viewed as critically vulnerable. It is unclear, given the history here as well as the SOS's new contract with Dominion, what this change actually encompasses. The voter registration database, containing millions

of Georgia voters' personal identifying information, plays a vital role in the proper functioning of the voting system. Yet it has been open to access, alteration, and likely some degree of virus and malware infection for years, whether in connection with: CES/KSU's handling of the system and data and failure to address these circumstances upon transfer of CES's functions back to the SOS; failure to remediate the database, software and data system flaws and deficiencies; or exposure of the widespread access to passwords to the voter registration data system throughout the SOS, CES/KSU, the 159 counties, or the public via the virtual open portal maintained at CES/KSU. Most significantly, the programming and use of ballots in both the DRE and future Dominion BMD system is tied to the accuracy of voter precinct and address information. Inaccuracy in this voter information thus triggers obstacles in the voting process. New Dominion express poll machines bought as part of the new contract with Dominion cannot alone cleanse the voter database to be transferred and relied upon.

In sum, the Court recognizes that the Secretary of State's Office and its leadership have likely benefited from the information provided in the Fortalice evaluations. Hopefully, this information translates into true intervention. All told, though, the picture remains that in the current cyber environment, the *present* voting system and voter registration database and system, as constituted and administered by the SOS and counties, bear critical deficiencies and risks that impact the reliability and integrity of the voting system process. The transference of defective voter data from one express poll electronic gateway to another one (whether or not the software is PCC's or Dominion's) remains a formidable obstacle to essential change of the voting system. [70] If voters' capacity to cast votes are thwarted through an inaccurate express pollbook voting check-in or voter website, this burdens their right to cast votes, scrambles election day voting procedures, and ultimately, in turn affects voting results.

F. The experience of voters in the 2018 election demonstrates serious problems and failures in the State's DRE/ GEMS and ExpressPoll systems.

***37** In support of their 2019 preliminary injunction motions, Plaintiffs provided affidavits from 137 Georgia voters, two county poll workers and fifteen poll watchers describing a variety of problematic issues with the voting process in the November 2018 general election. [71] (Docs. 412 and 413, Ex. A.) Voters, county election officials, and poll watchers described problems with the voting process in several Georgia counties, including Baldwin, Bleckley, Carroll, Chatham, Cherokee, Clarke, Clayton, Cobb, DeKalb, Dougherty, Early, Fayette, Fulton, Gwinnett, Henry, Meriwether, Muskogee, Paulding, Richmond, Thomas, Warren, Webster, and Wheeler counties. Reported problems included self-casting ballots, DRE machine malfunctions, voters' candidate selections flipping to other candidates on the DRE screens, and ballots being cast without a chance for the voter to review his or her selections. [72] Some DREs were taken out of service due to malfunction or irregularities, resulting in long lines at polling places, with many voters appearing to leave the polls without casting a vote. Countless voters also described issues with the electronic pollbook, such as an incorrect polling place or an incorrect address for the voter.

***38** Eighteen voters described seeing their vote selection on the DRE machine change from the candidate they selected to another candidate. (Doc. 412 at 44-84: Adams Aff.; Aldridge Aff.; Awan Aff.; Bish Aff.; Brison Aff.; Fennoy Aff.; Francois Aff.; Holt Aff.; Kelsey Aff.; Lee Aff.; Lester Aff.; Millet Aff.; Morris Aff.; Nichols Aff.; Sudden Aff.; Traylor Aff.; Williams Aff.; Worthy Aff.) These problems occurred on DRE voting machines in Bleckley, Henry, DeKalb, Gwinnett, Fulton, Meriweather, Cobb, Wheeler, Early, Warren, Chatham, and Paulding counties. Voters reported errors in their candidate selections for the Lt. Governor, Governor, and Insurance Commissioner races specifically. Many of these voters saw the machine switch the candidate during voting, while a number of them only noticed the change on the final review screen before casting their ballots. Eleven of these voters reported the issues to their poll workers. [73] No voters could verify whether their intended votes for particular candidates were actually cast, as the DREs in use in Georgia provide no audit trail or printout for voters to review for confirmation purposes.

Teri Adams described that when she voted at the Bleckley County Courthouse and selected candidate Stacey Abrams for governor on the DRE screen, she noticed that her designated selection was listed as Brian Kemp on the review screen. (*Id.* at 44.) She tried to vote for Abrams a second time, but the review screen again showed Kemp as her chosen candidate. Ms. Adams cast her ballot on the third try when her selection in the governor's race remained Abrams. Adams reported her problems on "machine number 2" to the poll workers whose only response was "did it take your vote?" (*Id.*)

When Amari Fennoy voted in Fulton County, she selected Stacey Abrams for governor on the DRE machine, then noted that she "saw the machine switched [her] vote to Brian Kemp." (*Id.* at 56.) Ms. Fennoy stated that she had to "click" Abrams name three times before the machine displayed her intended selection. (*Id.*) Cherry Worth, a Fulton County voter, was forced to make her selections 3 times, reported the problem with her machine to a poll worker who told her they had already had to shut down two voting machines that were exhibiting problems. (*Id.* at 83.)

Shirley Francois, a DeKalb County voter, states that during her voting experience on election day, for the first race on the ballot she pressed the selection for the Democratic candidate but noticed "it immediately jumped to the Republican," and that this happened at least twice. (*Id.* at 58.) When she could not get the machine to work, Francois decided to see what happened when she selected the Republican candidate and the machine stayed on the Republican candidate. (*Id.*) Francois then changed her selection back to the Democratic candidate. She proceeded to make the remainder of her candidate selections on the ballot, and when she got to the end of the ballot, the final summary review page showed all Republican candidates whom she had not chosen. (*Id.*) Francois went back to the beginning of the ballot to change all her votes again, and again had to make her selections two or more times before the machine would accurately reflect her chosen candidates. (*Id.*) Eventually, Francois was able to cast her ballot, but was left concerned at the amount of effort required of her to vote using the malfunctioning machine. (*Id.* at 59.)

Claudine Kelsey voted during the early voting period in Cobb County on October 19, 2018. (*Id.* at 62-63.) Her voting machine repeatedly changed her vote to candidates she did not choose. (*Id.* at 62.) When Kelsey pressed her choice for governor using the touchscreen DRE voting machine, the selection automatically changed to the person she did not choose. (*Id.*) She tried a second time, and the screen reflected the wrong candidate again. (*Id.*) On the third attempt, the screen correctly showed her selection. (*Id.)* After Kelsey made all of her selections, she double-checked the review screen to ensure it reflected her intended votes. (*Id.* at 63.) However, she does not know if it really worked and was alarmed it took three attempts to vote for the candidate of her choice. (*Id.*) Kelsey attests that she experienced similar problems with the voting machine she used during the 2016 Presidential election. (*Id.*)

***39** Sheena Brison from DeKalb County indicated that when she got to the page of the ballot where she could begin selecting the candidates she wanted to vote for, she very carefully and deliberately selected Stacey Abrams for governor. (*Id.* at 52-54.) However, when Brison selected Abrams' name, the screen blinked quickly and then showed that she had selected Brian Kemp for governor. (*Id.* at 54.) Brison called a poll worker over to her voting machine for assistance, who "backed all the way out" so Brison could start from the beginning. (*Id.*) She was able to select Stacey Abrams on her second attempt to vote, and the summary screen at the end of the voting process accurately reflected her candidate selections. (*Id.*)

Similarly, Pamela Lee, who voted early in Wheeler County on November 1, 2018 experienced a malfunctioning machine and was unable to confirm that her vote had been accounted for. (*Id.* at 64.) When Ms. Lee selected Janice Laws for Insurance Commissioner, "the selection changed/jumped to a different candidate above Janice Laws." (*Id.*) She brought the issue to the attention of the poll worker who advised her to "back out of that selection and try again." (*Id.*) On the second try, Lee was able to cast her ballot. (*Id.*) Following the election, Lee attempted to confirm that her vote had been cast. As of November 15, 2018, the Secretary of State's "My Voter Page" did not show that her early vote had been cast. (*Id.*)

Five other voters described not being able to review their selections prior to the machine "self-casting" their ballot or not being sure if their ballots had been cast. Vernon Jones declared that he was a longtime voter and has always been able to review his votes, prior to permanently casting his ballot. (*Id.* at 35.) However, when he voted in Chatham County in 2018, the machine cast his ballot without giving him a chance to review his selections. (*Id.*) After Stephanie Sudden voted on a DRE in DeKalb County, she described that "the summary page reflected only some of my choices and I had to go back and re-select candidates again." (*Id.* at 77.) In addition, she stated after reviewing her choices, she "clicked 'Cast Ballot' and the machine clicked off." (*Id.*) Ms. Sudden brought her issue to the attention of a poll worker who indicated to Sudden that the poll workers "had been having problems with the machine all day." (*Id.*) Durga Shah and Grace Ann Young, both DeKalb County voters, had similar experiences with machines casting their ballot before they could review their selections. (*Id.* at 37-42.)

Several more voters experienced problems with their voter cards. Jesse James Morris, Jr., a Chatham County voter, attests that after he experienced problems with his voting machine changing his candidate selections, when he tried to correct his vote, "the card would not stay in the voting machine [and he] had to force it to stay in and hold it in." (*Id.* at 71.) As a result, Morris is not sure his vote was counted correctly. (*Id.*) Marcus Napper, another DeKalb County voter, explains in his affidavit that he was not permitted to complete the voting process. (*Id.* at 73-75.) While he was voting on the voting machine, Napper received a notification stating, "ballot did not register," indicating to him that his vote had not been cast or counted. (*Id.* at 73.) He called an election official over to flag the issue, who took his "voter card and put it into two other machines to verify" the card was working. (*Id.*) After seeing that the voter card was functioning on the other machines, the poll worker was satisfied that Napper's ballot had been submitted. (*Id.* at 74.) According to Napper, however, he was "not permitted to return to the voting machine" and was "never able to select [his] candidates and receive a confirmation that [his] ballot was received." (*Id.*)

***40** Twelve voters described DRE machines not working or malfunctioning. (*See* Mitchell Aff.; Hawkins Aff.; Lack Aff.; Maddox Aff.; Marion Aff.; Oatis Aff.; J. Young Aff.; U. Young Aff.' Williams Aff.; Fore Aff., Doc. 412 at 86-120.) Voters in Columbus-Muskogee, DeKalb, and Fulton counties voted on DRE machines that did not include the Lt. Governor's race on the ballot until the final review screen (and in one case not at all). (Polattie Aff., Doc. 412 at 10-12; Thomas Aff., Doc. 412 at 13-16; Talley Aff., Doc. 412 at 17.) Sharita Mitchell, a voter in Thomas County, voted on a machine that "flickered" and "glitched" on every screen, failed to record her candidate selections multiple times, and "glitched" again after she clicked the button to cast her ballot. (*Id.* at 100-101.) Mitchell informed a poll worker about the machine, but he did not express any concern. (*Id.* at 101.)

Nathaniel Lack who voted at the St. James United Methodist Church in Alpharetta, Fulton County, noticed a hand-written "Out of Order" sign next to the voting machine he was using that appeared to have been taken down. (*Id.* at 96-97.) After attempting to vote by following the instructions by touching the check boxes next to the candidate's names, Lack noticed that his votes were not being registered unless he continued to tap on the touchscreen farther and farther away from the check boxes until the vote was registered on the screen. (*Id.* at 96.) Lack notified a poll worker who indicated they were aware this particular machine was "broken" and that a voter must click in odd places along the candidate's name for the vote to be registered by the machine. (*Id.*) The poll worker indicated they put the sign up when they knew the machine was not working properly but took the sign down and put the machine back into service for voting when the lines began to form. (*Id.*) Although Lack's selections showed on the final confirmation screen, he is not entirely confident that his vote was counted properly because of all the problems he encountered with the machine. (*Id.* at 97.) Lack indicated that his precinct is typically a highly Republican precinct and that he often votes Republican. (*Id.*) As a "computer expert specializing in troubleshooting problems," Lack believes "the failure of this machine puts every vote cast on it and all other 'glitchy' machines in question." (*Id.*)

Another voter in Fulton County, Kimberly Williams, assisted Derrard Leverette, a friend who was visually impaired cast his ballot in addition to casting her own ballot. (*Id.* at 113-16.) After she completed Mr. Leverette's candidate selections for him, "the machine ejected the yellow voting card really quickly, but at the bottom of the screen, it said that the vote had not been recorded." (*Id.* at 115.) Williams then decided to try her own voter card. After she made all of her selections, the same thing occurred: "the machine ejected the yellow card really quickly but stated that [her] vote had not been recorded." (*Id.*) Williams explained the problems to a poll worker, was given two new voting cards for herself and Mr. Leverette, and went through the voting process again without any apparent error with the new cards. (*Id.*) Despite the lack of an obvious sign the votes had not been counted the second time around, Williams remained worried that the votes might not have been counted following her experience with the first set of voter cards. (*Id.*)

Forty-six individual voters described issues with the electronic pollbook, including voters not being listed as registered, wrong addresses listed for the voters, incorrect polling places, and listing voters as having already voted. Many of the voters were offered a provisional ballot, but several voters were not. Instead, a large number of voters were told that they had to go to a different precinct to vote. Some of these voters would not have had enough time to travel to the precinct shown on the voter rolls in time to cast a ballot before the polls closed. (*See, e.g.* Antonio Greene Aff., Doc. 412 at 175) (stating that poll worker informed him close to 7:00 p.m. that he was not registered at his current address and would need to travel to Smyrna to cast

a regular ballot); Dasia Holt Aff., Doc. 412 at 205 (attesting that she was told by poll worker that she would have to travel 45 minutes to Columbus but she could not take off additional time off work to travel to another precinct to vote and was not offered a provisional ballot).

***41** Six of these voters were shown in the registration system as having already voted when they showed up at the polls to cast their ballots. When Amy Hoover voted in Fulton County, she inserted her voter card into the DRE machine and received an error message. (*Id.* at 104.) When a poll worker looked up her registration information, her status had changed to "voted." (*Id.*) While the poll workers were assisting her, Ms. Hoover witnessed four other voters have "the same problem on the same electronic voting machine." (*Id.* at 104.) Hoover and the other voters were told they could continue to wait or return in a few hours. (*Id.*) When she returned a few hours later, the system still showed Hoover's status as having voted. (*Id.*) According to Hoover, the poll workers were able to over-ride her status using the "master controller." (*Id.*)

On October 31, 2018, Cassandra Hollis attempted to assist her elderly mother, Tommie Hollis, with early voting. (*Id.* at 197-204.) Her mother, who had been recovering from a respiratory illness, had not left their home from September to October, other than to attend a few medical appointments. (*Id.*) However, when Hollis and her mother showed up at the C.T. Martin Natatorium in Atlanta to both vote on October 31st, they were told that Tommie Hollis had voted absentee in person at that same location on October 16th. (*Id.*) Hollis and her mother complained to two poll workers that this was a mistake. (*Id.* at 198.) Tommie Hollis, who was formerly a poll worker knew to call the Fulton County Board of Elections office. (*Id.*) The gentleman from Fulton County indicated there was nothing to be done because the system showed that Tommie Hollis had already voted. (*Id.* at 199.) Hollis herself started placing calls to see what could be done and was told by a friend to ask for a provisional ballot. (*Id.* at 200.) Tommie Hollis completed a provisional ballot and was given a document entitled "Notice to Provisional Voters from Fulton County Department of Registration and Elections Office." (*Id.* at 201.) Hollis made multiple calls to the Fulton County elections office from November 1 to November 9, 2018 in follow up to ensure that her mother's provisional ballot was properly counted. (*Id.* 201-202.) She left at least two detailed messages, but never received a response from anyone at Fulton County. (*Id.* at 203.)

According to Panessa Stephens's affidavit, when Stephens attempted to vote in person on November 6, 2018 at First United Lutheran Church in Cobb County – the polling place identified on the My Voter Page – he was told that he had been provided an absentee ballot and had already early voted. (*Id.* at 299-301.) The poll worker, Rick Martin, called the elections office and was informed that they had a record that Stephens had cast an absentee ballot at Jim Miller Park. (*Id.* at 300.) Stephens was instructed to cast a provisional ballot and Martin advised that the county would compare the signatures on the two ballots. (*Id.*) After casting the provisional ballot, Stephens called and spoke to someone in the Cobb County Elections Office and was notified that his in-person provisional ballot would be counted. (*Id.*) As of November 11, 2018, the Secretary of State's My Voter Page still showed Stephens as having cast an absentee/early ballot on October 25, 2018. (*Id.*)

Erin Himes from Fulton County, Elizabeth Murphy from Clarke County, and Mandi Herndon from DeKalb County also reported being told by poll workers that the system indicated they had each already voted when they had not. (*Id.* at 93, 193 244, 299.)

When Chris Duncan attempted to vote early in Fulton County, poll workers told him that his address in the voter registry did not match his driver's license address. (*Id.* at 155.) The address listed for him on the voter registry was from eight years prior. Mr. Duncan had confirmed his voter registration information on the Secretary of State's website prior to going to his polling place. After his attempt at early-voting, Mr. Duncan checked the website and found that his address had been changed on the site. When he went back to the polling place to vote on election day, poll workers told him that he had already voted by absentee ballot using his eight-year old address. (*Id.*)

***42** Voter Rodolfo Fadarjo moved to Carroll County three years before the 2018 election and changed his voter registration through the Georgia Department of Driver Services. (*Id.* at 160.) On election day, even though his wife was able to vote at the polling place in Carroll County, poll workers told Mr. Fadarjo that he was still registered at his old address in Paulding County. (*Id.*) Similarly, in Chatham County, Antoinette Johnson attempted to vote on election day after work. (*Id.* at 214.) He arrived at his polling place just before it closed along with his wife and daughter who reside at the same address where the family has

lived for two years. (*Id.*) Johnson's wife and daughter were allowed to vote, but Johnson was told he was at the wrong precinct and was not permitted to vote at his polling location. (*Id.*) Johnson did not get to vote because there was not enough time to travel to the other precinct before the close of the voting. (*Id.*)

Cobb County voter Christine Hanley and her daughter Annette went together to vote on election day at Crossview Baptist Church in Marietta where Hanley has voted for the last ten years, including in the 2018 primary election. (*Id.* at 190.) Ms. Hanley was told by a poll worker that her precinct was at Martin Luther King, Jr. Drive in Atlanta and that she would need to travel there to cast a regular ballot. (*Id.* at 191.) She explained to the poll worker that she had been voting at Crossview Baptist Church for a decade, but was only permitted to cast a provisional ballot. However, Hanley's daughter was able to cast a regular ballot. (*Id.*)

James Baiye of Gwinnett County attempted to vote in the November 6th election but was not permitted to vote because the registration system showed he had not voted in the two previous general election cycles and therefore was not properly registered to vote. (*Id.* at 124-25.) Baiye was not offered a provisional ballot. (*Id.*) According to Baiye, the information in the system was inaccurate because he voted by absentee ballot in the 2012 general election, and by direct vote in 2016. (*Id.*) Similarly, Ayesha Terry attempted to vote at the First Baptist Church in Henry County on election day, where she had voted in the 2016 Presidential election. (Doc. 413 at 15-17.) She was told her name was not in the system, that their records reflected an old address where she had lived in Macon, and that she had not voted for the last eight years. (*Id.* at 17.) Terry was not offered a provisional ballot and was unable to vote. (*Id.*)

Deborah Brown served as an Express Poll Clerk for the November 6, 2018 general election at the Coralwood precinct in DeKalb County. (*Id.* at 129-30.) Her duties as a poll clerk included requesting and receiving voter identification from voters, scanning voter identification cards, and providing voters with the yellow voter card for use in the voting machines. (*Id.* at 129.) At some point during the day Brown assisted a couple who came into the precinct to vote together. (*Id.*) They both provided identification showing they resided together at the same address. (*Id.*) When Brown scanned the female voter's identification first, the scan of the address showed her to be at the proper precinct for voting. (*Id.*) The scan of the address of the male voter's identification card showed that he was to vote at a different precinct. (*Id.*) Brown provided the male voter a provisional ballot rather than instructing him to go to a different precinct. (*Id.*) The fact that this couple, with the same address, had different voting precincts caused Brown concern over the integrity of the voting records. (*Id.*) [74]

Liza Niederwanger attempted to vote in Chatham County on election day at the Jewish Educational Alliance polling location. (*Id.* at 254-56.) The poll workers were unable to locate her information in the voter registration database even though she had her voter registration card issued by the Secretary of State, her valid driver's license, and a screenshot as proof of her registration from the Secretary of State's office. (*Id.* at 254.) She was given a provisional ballot to complete. (*Id.*) The next day Niederwanger went to the Voter Registration office in Savannah where her information was immediately found in the system. Still concerned, she visited the Board of Elections office next door. A supervisor located the envelope containing her provisional ballot and explained that the code assigned to her ballot indicated that she did not have identification. After Niederwanger explained that was a mistake because she had shown valid identification, the supervisor corrected the code to reflect that her registration could not be located. (*Id.* at 255.)

***43** Audrey Jackson worked as an Assistant Manager at precinct 082 in Gwinnett County and was responsible for calling the Gwinnett County Board of Elections with voting issues. (*Id.* at 209-210.) While serving in that capacity on election day, Jackson witnessed a number of issues that impacted individuals attempting to vote. (*Id.* at 209.) These issues included "having to turn voters away and they couldn't vote with provisional ballots, and system problems where voter cards reflected that the individual had already voted when they had not[,] ... voter registration applications that were never processed via email or online, and voters being told their registration would be processed after election day." (*Id.*) One voter, Gahalam Matz of Richmond County, was told he was listed as deceased and was not permitted to cast a ballot. (*Id.* at 236-238.) Another, Keteria Neal from Cobb County, was erroneously listed as having a felony preventing her from casting a regular ballot. (*Id.* at 251-53.) She was given a provisional ballot, but as of November 13, 2018 she still did not know the status of her ballot or whether her registration status had been corrected. (*Id.* at 253.)

Twenty-four voters and several poll watchers also described long lines at polling places, some of which were due to non-functioning DRE machines. Jeffery Young arrived at his assigned polling place in Gwinnett County to find that the "the machines were down." (*Id.* at 117.) He waited in line for four hours before being able to cast a ballot. (*Id.; see also* Oatis Aff., Doc. 412 at 108-114 (stating that none of the DREs in one polling place in Gwinnett County were reading the voter cards when the polls opened at 7:00 a.m., that new voter cards were brought in at 9:40 a.m., but that a large number of voters had already left the polling place).)

The Coalition Plaintiffs submitted similar evidence in their earlier 2018 preliminary injunction motions recounting voter problems with DRE voting machines and electronic pollbook errors occurring in connection with elections preceding the November 6, 2018 general election. (*See, e.g.*, Bowers Aff., Doc. 258-1 at 62-77; Mitchell Aff., Doc. 258-1 at 286-95.)

Laurie Aderholt Mitchell, a registered voter in Fulton County, has been registered to vote at her address on E. Wesley Road in Atlanta since June 2015. (Doc. 258-1 at 286.) Her husband Mark Mitchell is also registered to vote at the same address. (*Id.*) Ms. Mitchell was surprised to receive a new voter registration card in the mail on July 18, 2018 notifying her that her polling place had changed from the Cathedral of St. Phillip on Peachtree Road to Sutton Middle School on Northside Drive. (*Id.* at 286-87, 290-291.) Her husband had received no such notice of change in his polling place. (*Id.* at 287.)

Based on her review of recent news of problems with voter registration rolls, Mitchell visited the My Voter Page on the Secretary of State's website on July 19, 2019 to verify that the card she had received in the mail matched the online information. (*Id., see also id.* at 293.) She noticed that not only had her precinct location changed, but her precinct assignment had also changed from 08H to 07F. (*Id.*) Laurie Mitchell and her husband each checked their registration information on the My Voter Page and noticed that she was assigned to City Council District 8 while he was assigned to City Council District 7. (*Id.; see also id.* at 295.) The City Council District maps show that they live in District 7. (*Id.*)

Dana Bowers has been voting in Georgia elections since 2002 and is currently a registered voter in Gwinnett County where she has been registered at the same address since 2013. (*Id.* at 62.) In 2018, she worked as the Advocacy Coordinator in candidate Josh McCall's campaign for the 9th Congressional District. (*Id.*) One of Bowers's responsibilities for the campaign included monitoring potential voting problems in the 9th Congressional District. (*Id.*)

In that role, Bowers encountered issues with missing races on the DRE result tape from one voting machine (serial number 291032) in Hall County Precinct 10 during the May 22, 2018 primary election. The missing races included:

***44** • U.S. Representative, District 9 - REP

• U.S. Representative, District 9 - DEM

• State Senator, District 49 - REP

• State Representative, District 30 - REP

• State Representative, District 30 - DEM

• District Attorney, Northeastern Circuit - REP

• Solicitor General - R

• County Commissioner P1 - R

• County Commissioner P1 – D

(*Id.* at 63.) Poll workers certified all results tapes for all machines used, including the tape from the machine with the missing races. (*Id.* at 64.) Bowers requested public records related to the discrepancy and was informed that the "likely cause for the missing races is that the problem machine tape may have failed to engage and print a portion of the results," though there is no way to verify the cause of the problem or explain why the election results were certified in light of the malfunction of the machine. (*Id.* at 68.)

Similarly, while voting in Gwinnett County Precinct 100 in the July 2018 runoff, Bowers observed one DRE machine (serial number 291429) was marked "Do Not Touch" and was not in service. (*Id.*) She inquired about the machine and was told by Ms. Williams, a poll worker, that the machine "froze a few times" earlier in the day, and the poll manager discontinued its use for the remainder of the election. (*Id.* at 69.) Bowers asked whether the machine had been used by voters to cast votes before it was taken out of service and Williams confirmed that the machine had been used by voters for approximately "an hour to an hour and a half" after the polls opened at 7:00 a.m. (*Id.*) The poll manager, Denise Sullivan, however, told Bowers that voters had not cast votes on the machine. (*Id.*) When Sullivan decided to stop using the machine, the voter who was using the machine at the time was given a provisional ballot. (*Id.*) Bowers did not understand why the voter was not allowed to use a different DRE machine rather than being given a provisional ballot. (*Id.*)

After the closing of the polls at 7:00 p.m., Bowers overheard the poll workers talking about two machines "for which the tabulations were not reconciling." (*Id.* at 70.) She went outside the polling place with the poll manager and took photographs of the DRE machine results tapes including machine number 291429 after they were posted on the door at 8:40 p.m. (*Id.*) at 71.) The results tape for the machine showed no votes tallied and the results tape was attached to a "Zero tape" used at the opening of the polls to show that no votes are stored in the machines memory when voting begins. (*Id.*) Both opening zero report and the closing results tape displayed the identical printing time of 7:42 a.m. with no votes recorded for any candidate. (*Id.*) This was puzzling to Bowers because machine reports should be printed both before the 7:00 a.m. opening of polls and immediately after the 7:00 p.m. closing of the polls. (*Id.*) The machine results tapes for other machines showed print times ranging between 7:29 p.m. to 7:36 p.m., consistent with the time of day Bowers observed poll workers printing the results tapes after voting concluded.

***45** Concerned by recent reports and observations during voting in the May 2018 primary problems, Bowers decided to verify her voter registration status before voting on July 24, 2018. (*Id.* at 72.) Bowers checked her voter registration and polling place location on the My Voter Page on the Secretary of State's website, which indicated that her precinct number had changed to Precinct 100 though she had received no notice of such change. (*Id.*) Her precinct had long been Precinct 96, but she assumed the change was legitimate and authorized. (*Id.*)

Bowers arrived at Precinct 100 at approximately 6:20 p.m. and completed her voter application form and presented her driver's license to the poll worker. (*Id.*) Christine, the poll worker located Bowers in the electronic pollbook but informed her that she was in the wrong precinct and was supposed to vote in Precinct 96. Bowers explained that she had checked her registration on the Secretary of State's website that morning which showed her assigned precinct as Precinct 100. (*Id.* at 73.) Another poll worker, Carolyn Williams, stated that "this has been happening all day" and that she was aware of approximately 50 voters who had been assigned the wrong precinct. (*Id.*) Christine suggested that Bowers vote a provisional ballot given that there was not enough time to get to Precinct 96 before the polls closed at 7:00 p.m. and assured Bowers that the provisional ballot would be counted.

At 8:55 p.m. that evening, Bowers checked her voter registration page again on the My Voter Page and captured screenshots of the page showing the Precinct 100 assignment. (*Id.*) Several days later, at 7:24 p.m. on July 29, 2018, Bowers again checked her My Voter Page to see that her precinct assignment was this time showing her original Precinct 96. (*Id.* at 74.) She captured a screenshot of this change in status. Bowers had not made any changes to her voter registration. (*Id.*)

Through her work on the 9th Congressional District campaign, Bowers researched dozens of registration records for voters who reported being assigned to the wrong Georgia House District and reported receiving incorrect ballots in Habersham, Banks, Stephens, Franklin and Jackson counties in the May 22, 2018 primary. (*Id.* at 74-75.) She personally reviewed numerous discrepancies between the various voter assignment records for voters in counties in the 9th Congressional District. (*Id.* at

75.) As a result of this work and her own personal voting experience in July 2018, Bowers has significant concerns about discrepancies in the pollbooks and voter registration database and its burden and potential impact on voters' rights (including her own) to cast ballots for the correct candidates in their assigned districts and to have their votes counted. (*Id.*)

The Court also takes judicial notice of the evidence submitted by numerous voters and poll watchers in the *Common Cause v. Kemp* post-election challenge before the undersigned in November 2018. This evidence included sworn declarations of voters (and poll watchers) who faced hurdles in their registration status and even in obtaining the opportunity to cast provisional ballots at the polls after they were affirmatively told they were not on the registration rolls, despite having voted from the same home in the recent past or affirmatively representing they had timely registered and were regular voters. Repeated inaccuracies were identified in the voter registration system that caused qualified voters likely to lose their vote or to be channeled into the provisional voting process because their registration records did not appear or had been purged from the data system. For example, there was evidence from voters that they were registered but were told they were not in the registration system; there was evidence that voters were sometimes refused provisional ballots or sometimes only provided provisional ballots after returning to the polls to insist on this. Similarly, there was evidence from Common Cause poll monitors and hotline workers to the same effect.

***46** The evidence from both the 2018 and 2019 motions also indicates that this same pattern of problems with Georgia's voting systems and registration databases has persisted across multiple elections cycles. The evidence of the specific problems with the DREs experienced by a number of voters ties back into the expert studies detailing the various types of malfunctions (including software and miscalibration issues) found to occur during examination of the machines during the experts' rigorous testing described above.

IV. PLAINTIFFS' REQUESTED INJUNCTIVE RELIEF AND FEASIBILITY OF IMPLEMENTATION OF PAPER BALLOTS IN 2019 ELECTIONS

The Curling and Coalition Plaintiffs seek to (1) enjoin Defendants from using the Diebold AccuVote direct recording electronic ("DRE") voting system to conduct further elections in Georgia, including providing programming and machine configurations employing the DRE voting system; (2) require Defendants to conduct in-person voting in elections by hand-marked paper ballot [75] tabulated either by hand or by optical scanners; [76] (3) require the State Election Board and/or the Secretary of State to develop a proposed plan for immediate implementation of pre-certification, post-election, manual, tabulation audits of paper ballots as provided in O.C.G.A. 21-2-498; and (4) require the State Election Board and/or the Secretary of State to develop procedures to (a) address errors and discrepancies in the voter registration database and (b) provide for use of an updated paper backup of the pollbook in all polling places for adjudicating voter eligibility and precinct assignment problems.

In addition, the Coalition Plaintiffs request separately that the Court Order: (1) require Defendants to take necessary action to maintain ballot secrecy; (2) require the State Election Board to propose a plan for auditing elements of DRE elections, including pre-certification audits of election results and pre-certification audits of the computer-generated tabulations of absentee mail ballots and tests of DRE output accuracy; (3) require Defendants to immediately instruct every Election Superintendent to direct that all precinct level poll officials inform voters who are denied a regular ballot of their right to cast a provisional ballot; and (4) require Defendants to develop and implement a plan to undertake a security evaluation of the Secretary of State's election servers and counties' GEMS servers and other voting system components, including electronic pollbooks, to detect malware or other significant security vulnerabilities and develop appropriate mitigation action and timetables.

***47** The State Defendants' opposition to the implementation of Plaintiffs' request for a paper ballot election system is two-fold: first, it would be too costly and burdensome to be feasible; and second, it would be too disruptive in the interim while the State is simultaneously transitioning to the new BMD system and is therefore not in the public interest.

The State Defendants assert that the public interest in orderly elections does not favor spending enormous amounts of time and money on a system that will be used only for municipal elections in 2019. [77] They further assert that the costs and burdens

imposed on State elections officials and the taxpayers would be significant and distract the State in its process of transitioning to a new voting system that eliminates DREs by the March 2020 primary. [78] The State Defendants contend that Plaintiffs' request for a move to paper ballots before the State implements the newly passed voting system is not feasible because: (1) "the full scope of the costs to the State Defendants (as opposed to the local elections officials who are statutorily responsible for the elections) is difficult to quantify" and (2) "Georgia's municipalities conducting elections will be the ones who bear the brunt of Plaintiffs' proposed relief." (State Defs.' Resp. at 55.) [79]

A. Defendants' Evidence

***48** Although the State Defendants argue that implementing a temporary system for the November 2019 elections will impede the state's ability to implement a new voting system – they presented no witness to provide any evidence at the hearing about the Secretary of State's implementation schedule or progress. Nor did the State Defendants present any witness or evidence regarding how the Curling Plaintiffs' proposal, which includes implementing a significant portion of the State's new election system – one BMD per precinct for disabled voters along with the new optical ballot scanners – would interfere with the State's orderly implementation.

Defendants presented testimony from election administration officials in three counties that will be conducting county or municipal elections in the Fall: Chatham, Fulton, and Morgan counties. [80]

Russell Bridges, Supervisor of Elections for Chatham County since 2004, provided testimony regarding the feasibility of using hand-marked paper ballots in lieu of DREs for the scheduled elections. The Chatham County Board of Elections conducts elections for all eight municipalities in Chatham. (Bridges Decl., Doc. 472-6.) Six of these cities will conduct elections on November 5, 2019, including Garden City, Pooler, Port Wentworth, Savannah, Tybee Island and Vernonburg.

Chatham County will also be conducting a countywide SPLOST referendum on November 5th. There are 207,000 active registered voters in Chatham County, and the Board of Elections intends to use 90 voting precincts throughout the County. Bridges testified that "in a typical election, the concentrated preparation is about eight weeks of actual" preparation time when his teams prepare equipment, prepare the ballots, and train poll workers. (Tr. Vol.2, Doc. 571 at 250.) Chatham County is planning to conduct the November elections using DREs. Early voting begins October 15th.

Mr. Bridges testified that he does not believe Chatham County has sufficient funds in the existing elections budget for 2019 to purchase new equipment for a paper ballot system. (*Id.* at 257.) His entire budget for 2019 is $1,073,000. (*Id.* at 269.) If the Court required Chatham County to use paper ballots, Mr. Bridges stated the purchase of additional equipment and paper ballots could cost anywhere between $500,000 to $950,000. [81] (Bridges Decl., Doc. 472-6 at 7-9; *see also* Tr. Vol.2, Doc. 571 at 262, 270.) Currently the DRE elections in Chatham County typically cost $185,000 total. (*Id.* at 266.)

***49** Mr. Bridges testified that he would need a minimum of 90 optical scanners – one scanner per precinct – but his preference would be to have a stock of 30 to 50 back up scanners in case some equipment does not work. (*Id.* at 259-260, 265.) He therefore estimates Chatham County would need approximately 130-140 scanners to account for the anticipated fifty percent voter turnout. [82] (*Id.* at 261, 265; *see also* Bridges Decl., Doc. 472-6 at 7.) Chatham County currently has only 8 optical scanners that are roughly 25 years old. (Tr. Vol.2, Doc. 571 at 264.) Mr. Bridges testified he would need to print between 125,000 to 175,000 ballots at a cost of 50 cents a ballot, for total cost between $60,000 to $100,000. (*Id.* at 266; *see also* Bridges Decl. at 6.)

Richard Barron, the Director for the Fulton County Board of Registration and Elections, testified that Fulton County does not have an elections budget during odd-numbered years, it only has an operating budget, and that there is about $1 million dollars remaining in the operational budget for 2019. [83] (Tr. Vol.2, Doc. 571 at 210.) He further testified that when the County conducts municipal elections, the municipalities pay for those elections. (*Id.*) Fulton County expects to receive approximately $1.1 million from the ten municipalities for the elections the County will be conducting in November. (*Id.* at 229.)

The City of Atlanta is not currently scheduled to hold any elections in November. (*Id.* at 224.) Fulton County will conduct two elections for the City of Atlanta on September 3, 2019 for County Commission District 6 and Atlanta Public School Board District 2. Early voting for these elections begins August 26, 2019 and absentee ballots will begin to be mailed on August 26, 2019. (Decl. of Joseph Blake Evans, Doc. 473-1 ¶¶ 10, 14.) Ten other municipalities in Fulton have elections scheduled in November, including: Alpharetta, College Park, East Point, Fairburn, Hapeville, Johns Creek, Milton, Roswell, South Fulton, and Union City. (Doc. 537-3 at 12-13; Municipality Elections Chart.)

Mr. Barron testified that Fulton Co. would need 130 optical scanners that are compatible with the GEMS system for the September election. (Tr. Vol.2, Doc. 571 at 212.) Fulton County currently has 36 scanners (which are used to centrally scan absentee ballots) and would need to purchase 94 additional scanners. (*Id.*) If there was a budgetary issue, Barron testified that Fulton County could use its existing scanners to do a central count of the paper ballots for the Fall 2019 election cycle. (*Id.* at 236-37.) In addition to purchasing additional optical scanners, Mr. Barron stated that to conduct an election on paper, the county would have to train poll workers who are unfamiliar with scanning paper ballots at the precinct level, [84] and procure ballot boxes, cabinets to store the paper ballots, and voting booths. (*Id.* at 219-22, 229.)

Mr. Barron estimates there will be between 16,000 to 20,000 voters in the two September City of Atlanta races. (*Id.* at 233.) In November 2018 election Fulton County processed between 18,000 and 22,000 hand-marked paper ballots (absentee and provisional). For the November 2019 election, he estimates the voter turnout will be much less than the same election cycle in November 2017 because the City of Atlanta will not be conducting any elections and it typically has a much higher turnout than other municipalities. He would estimate between 5 to 12 percent of voters in November 2019 – which would be about the same number total of absentee ballots processed by the County in the November 2018 election. (*Id.* at 233-34).

***50** Defendants also presented Jennifer Doran, the Elections Supervisor for Morgan County, to provide testimony about the feasibility of implementing a paper ballot system for the November 2019 elections. Morgan County has 14,000 registered voters and an elections budget for the fiscal year July 1, 2019 to June 30, 2020 of $30,000 (excluding salaries for staff and poll workers). Morgan County conducts all municipal elections in the county through intergovernmental agreements that provide that the municipalities reimburse the county for actual costs associated with the election. (July 26, 2019 Tr., Doc. 571 at 320-21.) Morgan County has four municipalities, with three cities scheduled to conduct elections on November 5, 2019. (*Id.* at 319-20.) The number of registered voters expected to turnout in the three municipalities could be anywhere from 1,020 to 2,220 voters. (*Id.*)

Ms. Doran testified that if Morgan County were required to switch to a paper ballot system, it is her understanding the county would be responsible for paying for the purchase of new equipment. (*Id.* at 321.) According to Ms. Doran, if all of the municipalities held elections, Morgan County would need four optical scanners with ballot boxes at a cost of $5,000. [85] (*Id.*) This additional money is not in the current budget, which is already very lean. (*Id.* at 321.) Morgan County currently has only two optical scanners. (*Id.* at 327.) The Morgan County Board looked at the feasibility of moving to paper ballots in August or September of 2018. Ms. Doran determined what the necessary budget number would be and contacted their vendor, ES & S, and received a quote of $1,300 per optical scan unit with ballot box for the same equipment currently used by Morgan County. (*Id.* at 322.) Other than the purchase of more scanners, additional costs include: a few hundred dollars in cost of printing ballots at 40 cents per ballot and pay for the additional man-hours for a different arrangement of staff (but with the same staff she currently uses to conduct elections). (*Id.* at 322-23, 330, 336.)

To implement the change in time for the election, Morgan County would need to have all equipment and supplies ready in October. (*Id.* at 323.) Once new scanners are purchased, they must also go through certification and testing by the Secretary of State. According to Doran, the last time Morgan County bought new equipment, the turn-around time from the Secretary of State was two months. (*Id.*) Doran testified that it is feasible to do a hand-count of paper ballots, but it would take longer to tabulate the votes after the election. (*Id.* at 328.)

None of the elections officials who testified accounted for the cost and time savings of not having to prepare and test the DREs.

B. Plaintiffs' Evidence

Plaintiffs presented testimony from numerous elections officials with experience transitioning from electronic voting systems to paper ballots. These include Amber McReynolds, former Director of Elections for the city and county of Denver, Colorado; Virginia Martin, Election Commissioner for Columbia County, New York; Lowell Finley, the California Deputy Secretary of State for Voting Systems Technology and Policy from 2007-2014; Candice Hoke, Professor of Law at Cleveland State University and former Director for Election Integrity for Cuyahoga County Ohio (inclusive of Cleveland); and Rebecca Wilson, Republican/Unaffiliated Chief Election Judge in Prince George's County, Maryland. [86]

***51** Lowell Finley, California Deputy Secretary of State for Voting Systems Technology and Policy from 2007-2014, testified on behalf of the Curling Plaintiffs. [87] In that capacity, Finley oversaw and administered the drafting of voting system standards for California, oversaw the state voting system certification process, was responsible for standards for ballot printers in the state, and in the first year of 2007 was responsible for designing and administering a statewide review of all electronic voting systems that were in use in the state. (Tr. Vol. 2, Doc. 571 at 34.)

After a several-months long study conducted by top computer science professors and experts around the country of California's DREs, California's Secretary of State decertified tens of thousands of DREs affecting 4.3 million voters. (*Id.* at 37.) Finley testified that California made the transition from DREs to paper ballots over a 6-month period for use in the dozens of counties statewide that had been using DREs in time for the 2008 Presidential Primary. [88] (*Id.* at 76.)

According to Mr. Finley, there are elements of Georgia's new planned election system, which can be leveraged to implement a system in time for the Fall 2019 elections that does not rely on DREs. Using the scanners that are proposed in the State's new legislation along with a single ballot marking device for each polling place to provide for voters with disabilities, [89] Finley testified it would be possible to deploy a system that relied primarily on hand-marked paper ballots. (*Id.* at 46.) More specifically, with Georgia's plan to pilot using optical scanners in several counties in November and then only seven weeks later, provide all counties with precinct level optical scanners, the system could be put in place for the limited number of precincts that are going to be conducting elections in November. (*Id.* at 47-48.) Because Georgia has already embarked on its process of implementing an entirely new system "on a very aggressive schedule," and the work is already underway, Finley believes it is feasible for Georgia to advance the procurement process and timeline in order to acquire enough scanners to supply to the precincts participating in the November elections. (*Id.*)

The Coalition Plaintiffs offered testimony from the former Director of Elections for Denver, Colorado. As Director of Elections for Denver, Amber McReynolds [90] oversaw the transition from a primarily DRE-based election system to a primarily hand-marked paper ballot system, which occurred from 2005 to 2007. (Tr. Vol.1, Doc. 570 at 117-18.) She also implemented a change to risk-limiting audits after Colorado passed election reform legislation in 2013. (*Id.* at 119.)

Ms. McReynolds testified that the feasibility issues that Georgia would face in transitioning from DREs to paper ballots are similar to what they faced in Colorado. (*Id.*) ("[T]he feasibility in terms of the hardware equipment systems and sort of transitioning to a new system are similar complexities to what exists anywhere really in the country.") Because Georgia already uses paper for absentee and provisional ballots, McReynolds testified the transition is easier. (*Id.* at 128) ("[W]hen you are already doing mail ballots and you already have to process and centrally count those ... the transition to paper ballots becomes much easier. It isn't that much more to add basically the paper coming from all of the polling locations.") (*Id.*)

***52** From both an efficiency and security standpoint, McReynolds prefers central count scanning for paper ballots over precinct count scanning. (*Id.* at 129.) According to McReynolds there is a significant cost savings by not using DREs. (*Id.* at 157) ("[W]hen you factor in the cost of, you know, less equipment, less delivery, all of that, coupled with the cost of the ballot

printing, you actually see more of a savings when you are not having to have as much equipment out in the field and process all of that out in the field.").

Based on her experience, McReynolds is concerned that the major transition to BMDs that is planned in Georgia is not as feasible in the timeframe projected by the State and is concerned about Georgia's use of DREs as their fall back if there are problems with timely implementation of BMDs. In her declaration, she stated that to the best of her knowledge, Georgia's planned transition to an electronic touchscreen BMD system by March 2020 "would be the largest and most complex voting system conversion ever attempted in the nation in such a short time frame," and that "[t]he continued use of the current unauditable DRE system should not inadvertently become the 'back up plan' for failure or delays that may occur while attempting to purchase and implement a new voting system." (Doc. 413, Ex. D at 222, ¶¶ 4, 9.)

Dr. Virginia Martin, the Election Commissioner for Columbia County, New York who was responsible for overseeing a transition to hand-marked paper ballots and optical scanners in 2009 and 2010 also testified on behalf of Plaintiffs at the preliminary injunction hearing. (Tr. Vol. 2, Doc. 571 at 7-32.) Dr. Martin made the transition in three months from the time a Court order was issued in June 2010 until a pilot in Columbia county in September 2010. (*Id.* at 10.) Dr. Martin testified that she has assisted other jurisdictions including in Colorado and Rhode Island, make similar transitions and that that the core foundational elements of running an election with hand-marked paper ballots are the same everywhere. (*Id.* at 11, 13.)

Finally, the Coalition Plaintiffs submitted the declaration of Candace Hoke, Professor of Law at Cleveland State University, and former Director for Election Integrity for Cuyahoga County Ohio [91] regarding the feasibility and security benefits of conducing Georgia's elections on an auditable and verifiable paper ballot system based on Georgia's current use of paper absentee ballots. [92] (Decl. of Candice Hoke, Doc. 413, Ex. E.) Professor Hoke founded the "Center for Election Integrity" at Cleveland State University in 2005. She also participated as a researcher in the California Secretary of State's scientific study of voting system security and provided guidance to the Ohio Secretary of State's office in structuring its own scientific study of voting system security in 2007. In Ohio, Hoke also at various times has served within the election administrative system in several capacities, including as a supervising poll worker, a "roving" election technology trouble-shooter, a voter registration problem-solver, and a consultant to the Ohio Secretary of State's Office on election management and improvement. (*Id.* ¶ 20.)

***53** While Professor Hoke was serving as the Director of the Center for Election Integrity, "Cuyahoga County experienced an internationally notorious election disaster when it sought to implement its new Diebold electronic voting system primarily comprised of DRE touchscreen units at polling locations, AccuVote scanners for absentee paper ballots, and the GEMS server" during the Federal Primary election in May 2006 when "[e]very technical and managerial system failed." (Decl. ¶ 11.) Hoke was appointed to the 3-member Cuyahoga Election Review Panel to investigate and evaluate the problems with the election system and the Center for Election Integrity was appointed to serve as Public Monitor of Cuyahoga Election Reform through 2008. She served as "Project Director of the Public Monitor" during that time, selecting, training, and supervising the work of an 18-person staff in investigation the causes and remedies for the failed 2006 Federal primary election. "By talking with election officials and election technology vendors from other jurisdictions, and reviewing documentary evidence," Hoke attests to gaining a "vast knowledge of markedly different activities undertaken by other jurisdictions which experienced decisive success in their e-voting transitions." (*Id.* ¶ 18.)

As Director of the Public Monitor of Cuyahoga Election Reform, Hoke assisted the County in determining whether to move from DRE voting machines to hand-marked paper ballots tabulated by optical scanners, and then, ultimately in transitioning to a new hand-marked paper ballot system using precinct-count scanning for in-person voting and central-count scanning for absentee ballot tabulation at the elections office. On December 21, 2007, while Hoke was serving as Public Monitor, Ohio's Secretary of State directed the Cuyahoga County Board of Elections to abandon its DRE touchscreen voting machine system in exchange for the optical scan voting system with hand-marked paper ballots by the March 4, 2008 Presidential Primary. (*Id.* ¶ 22.) Hoke initially had doubts whether 60 days was a sufficient length of time for such a transition, when it could have been implemented months earlier. (*Id.* ¶ 23.) However, the "highly motivated executive officials and capable staff" were able to lease state-certified optical scanners and successfully conduct the election with an auditable election record. (*Id.* ¶¶ 23-24.)

According to Professor Hoke, it is not necessary for Georgia to overhaul the entire election management system and all its components. Instead, Georgia can merely expand the use of the existing GEMS system and Diebold AccuVote optical scanners paired with statistically-valid and robust post-election audits as a check for the vulnerabilities that cannot be otherwise mitigated in the current optical scan system. (*Id.* ¶¶ 25-34, 38.) Compared to the monetary cost of maintaining, transporting, storing, securing, and testing DRE machines, the cost of implementing a hand-marked paper ballot system is comparatively lower. (*Id.* ¶ 45.)

Professor Hoke is aware of Georgia's plan to launch its new voting system for use in the 2020 Presidential Primary election. (*Id.* ¶ 39.) "Generally, the rule in election administration is to roll out mission-critical new technology in off-year, non-federal election years, as the volume of voters and candidates/issues is normally smaller and thereby reduces the complexities that must be managed." (*Id.*) In her experience, Hoke attests, such off-year elections are more ideal for transition because they likely require fewer ballot styles and contain fewer election questions and races than a primary or general statewide election. (*Id.* ¶¶ 40-41.) For this reason, Hoke believes the 2019 municipal election cycle is the ideal time for Georgia to transition to a paper ballot system in these smaller scale elections. (*Id.* ¶¶ 41-42.)

V. ANALYSIS OF INJUNCTIVE RELIEF FACTORS

To obtain preliminary injunctive relief, the moving party must show that: (1) it has a substantial likelihood of success on the merits; (2) irreparable injury will be suffered unless the injunction issues; (3) the threatened injury to the movant outweighs whatever damage the proposed injunction may cause the opposing party; and (4) if issued, the injunction would not be adverse to the public interest. In the Eleventh Circuit, "[a] preliminary injunction is an extraordinary and drastic remedy not to be granted unless the movant clearly established the 'burden of persuasion' as to the four prerequisites." *McDonald's Corp. v. Robertson*, 147 F.3d 1301, 1306 (11th Cir. 1998). (internal citations omitted).

***54** This Court previously determined that Plaintiffs' evidence (even at the preliminary stage) established a substantial likelihood of prevailing on their claims that the State's failure to remedy known security breaches and exposures compromising Georgia's electronic voting machines and election servers violates their Fourteenth Amendment substantive due process and equal protection rights. Specifically, the Court found:

> Plaintiffs have shown that their Fourteenth Amendment rights to Due Process and Equal Protection have been burdened. Put differently, the State's continued reliance on the use of DRE machines in public elections likely results in "a debasement or dilution of the weight of [Plaintiffs'] vote[s]," even if such conduct does not completely deny Plaintiffs the right to vote. *Bush v. Gore*, 531 U.S. 98, 105, 121 S.Ct. 525, 148 L.Ed.2d 388 (2000) (quoting *Reynolds*, 377 U.S. at 555, 84 S.Ct. 1362).... Plaintiffs have so far shown that the DRE system, as implemented, poses a concrete risk of alteration of ballot counts that would impact their own votes. Their evidence relates directly to the manner in which Defendants' alleged mode of implementation of the DRE voting system deprives them or puts them at imminent risk of deprivation of their fundamental right to cast an effective vote (i.e., a vote that is accurately counted). *United States v. Classic*, 313 U.S. 299, 315, 61 S.Ct. 1031, 85 L.Ed. 1368 (1941); *Stewart*, 444 F.3d at 868. Plaintiffs' evidence also goes to the concern that when they vote by DRE, their vote is in jeopardy of being counted less accurately and thus given less weight than a paper ballot.

Curling v. Kemp, 334 F. Supp. 3d 1303, 1322 (N.D. Ga. 2018).

As discussed further below, the Court again finds that the Plaintiffs have continued to demonstrate a likelihood of prevailing on the merits of their claims that the current non-auditable Georgia GEMS/DRE voting system, as implemented, burdens and deprives them of their rights to cast secure votes that are reliably counted, as guaranteed under the First and Fourteenth Amendments of the United States Constitution. The threatened, ongoing injury here is an irreparable injury – one that goes to the heart of the Plaintiffs' participation in the voting process and our democracy. But the Court must also consider, in determining whether preliminary injunctive relief should be granted, whether the threatened injury to Plaintiffs outweighs whatever damage the proposed injunction may cause the Defendants; and, if issued, whether the injunction would not be adverse to the public

interest. And again, the Court must consider how Plaintiffs' requested injunctive relief during an interim cycle of elections could negatively impact the public's interest in the State's ability to marshal in a new election system – using electronic ballot markers that produce paper ballots tabulated using ballot scanners – in the coming months in time for the 2020 Presidential primary election cycle, which is the State's target deadline under the terms of its contract with Dominion.

"When a State exercises power wholly within the domain of state interest, it is insulated from federal judicial review. But such insulation is not carried over when state power is used as an instrument for circumventing a federally protected right." *Reynolds v. Sims*, 377 U.S. 533, 566, 84 S.Ct. 1362, 12 L.Ed.2d 506 (1964) (quoting *Gomillion v. Lightfoot*, 364 U.S. 339, 347, 81 S.Ct. 125, 5 L.Ed.2d 110 (1960)); *see also Lassiter v. Northampton Cty. Bd. of Elections*, 360 U.S. 45, 50, 79 S.Ct. 985, 3 L.Ed.2d 1072 (1959) ("The States have long been held to have broad powers to determine the conditions under which the right of suffrage may be exercised, absent of course the discrimination which the Constitution condemns." (citations omitted)). While the Constitution affords the states broad power to regulate the conduct of federal and state elections, "the federal courts have not hesitated to interfere when state actions have jeopardized the integrity of the electoral process." *Duncan v. Poythress*, 657 F.2d 691, 702 (5th Cir. 1981). [93]

***55** The Constitution of the United States "undeniably" "protects the right of all qualified citizens to vote, in state as well as in federal elections." *Reynolds*, 377 U.S. at 554, 84 S.Ct. 1362. Voting is, indisputably, a right " 'of the most fundamental significance under our constitutional structure.' " *Burdick v. Takushi*, 504 U.S. 428, 433, 112 S.Ct. 2059, 119 L.Ed.2d 245 (1992) (quoting *Illinois Bd. of Elections v. Socialist Workers Party*, 440 U.S. 173, 184, 99 S.Ct. 983, 59 L.Ed.2d 230 (1979)). And "[t]he right to vote freely for the candidate of one's choice is of the essence of a democratic society, and any restrictions on that right strike at the heart of representative government." *Reynolds*, 377 U.S. at 555, 84 S.Ct. 1362. State and local laws that unconstitutionally burden that right are impermissible. *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 451, 128 S.Ct. 1184, 170 L.Ed.2d 151 (2008).

Here, Georgia law requires a uniform statewide voting system for all federal, state, and county elections. Plaintiffs do not challenge the constitutionality of the Georgia election statute per se. Rather, they challenge Georgia's continued use of the chosen DRE/GEMS voting system pursuant to that law, which has been shown to operate on unsecure, unreliable and grossly outdated technology that jeopardizes their ability to cast votes that reliably and accurately will be counted or counted on the same basis as someone using another voting method. Plaintiffs have shown that the corrosion of the accuracy and reliability of the mandated electronic voter registration database and Express Poll system used at the polls in tandem with the DRE/GEMS voting system has seriously aggravated the arbitrary and unlawful character of Defendants' implementation of the State mandated voting system, in derogation of their First and Fourteenth Amendment rights. Plaintiffs have also shown the imminent risk of harm in the burdening or deprivation of these rights in the upcoming 2019 elections.

When deciding whether state-enacted election methods and procedures violate the Fourteenth Amendment, the Court must weigh the character and magnitude of the burden the State's rule imposes on those rights against the interests the State contends justify that burden and consider the extent to which the State's concerns make the burden necessary. *Timmons v. Twin Cities Area New Party*, 520 U.S. 351, 358, 117 S.Ct. 1364, 137 L.Ed.2d 589 (1997); *Burdick v. Takushi*, 504 U.S. 428, 434, 112 S.Ct. 2059, 119 L.Ed.2d 245 (1992) ("The Constitution provides that States may prescribe '[t]he Times, Places and Manner of holding Elections for Senators and Representatives,' Art. I, § 4, cl. 1, and the Court therefore has recognized that States retain the power to regulate their own elections."); *Anderson v. Celebrezze*, 460 U.S. 780, 788, 103 S.Ct. 1564, 75 L.Ed.2d 547 (1983) ("Although these rights of voters are fundamental, not all," state election laws, "impose constitutionally-suspect burdens on voters' rights ...."). Because the right to vote is fundamental and the exercise of that right "in a free and unimpaired manner is preservative of other basic civil rights, any alleged infringement of the right of citizens to vote must be carefully and meticulously scrutinized." *Reynolds*, 377 U.S. at 562, 84 S.Ct. 1362; *Democratic Executive Committee of Florida v. Lee*, 915 F.3d 1312, 1319 (11th Cir. 2019) (noting that the Supreme Court has "long recognized that burdens on voters implicate fundamental First and Fourteenth Amendment rights").

The Fourteenth Amendment due process clause protects against "the disenfranchisement of a state electorate." *Duncan*, 657 F.2d at 708. "When an election process 'reaches the point of patent and fundamental unfairness,' there is a due process violation." *Florida State Conference of N.A.A.C.P. v. Browning*, 522 F.3d 1153, 1183–84 (11th Cir. 2008) (quoting *Roe v. Alabama*, 43 F.3d 574, 580 (11th Cir.1995) (citing *Curry v. Baker*, 802 F.2d 1302, 1315 (11th Cir.1986))). And "[w]hen a state adopts an electoral system, the Equal Protection Clause of the Fourteenth Amendment guarantees qualified voters a substantive right to participate equally with other qualified voters in the electoral process." *Reynolds*, 377 U.S. at 566, 84 S.Ct. 1362; *see also Harper v. Va. Bd. of Elections*, 383 U.S. 663, 665, 86 S.Ct. 1079, 16 L.Ed.2d 169 (1966). In any state-adopted electoral scheme,

> ***56** [t]he right to vote is protected in more than the initial allocation of the franchise. Equal protection applies as well to the manner of its exercise. Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person's vote over that of another.

Bush v. Gore, 531 U.S. at 104–05, 121 S.Ct. 525; *see also Davis v. Bandemer*, 478 U.S. 109, 124, 106 S.Ct. 2797, 92 L.Ed.2d 85 (1986) (noting that "everyone [has] the right to vote and to have his vote counted"); *Democratic Executive Committee of Florida v. Lee*, 915 F.3d at 1319 (reiterating that voters enjoy a fundamental right under the Fourteenth Amendment "to participate equally in the electoral process"); *Stewart v. Blackwell*, 444 F.3d 843, 868 (6th Cir. 2006) ("All of the precedent indicates that having one's vote properly counted is fundamental to the franchise."), *vacated by* 473 F.3d 692 (6th Cir. 2007) (subsequently vacating appeal as moot after state's abandonment of election machines). [94]

"Just as the equal protection clause of the fourteenth amendment prohibits state officials from improperly diluting the right to vote, the due process clause of the fourteenth amendment forbids state officials from unlawfully eliminating that fundamental right." *Duncan*, 657 F.2d at 704. It is well established that when a state accords arbitrary and disparate treatment to voters, those voters are deprived of their constitutional rights to due process and equal protection. *Bush v. Gore*, 531 U.S. at 107, 121 S.Ct. 525 (citing *Gray v. Sanders*, 372 U.S. 368, 379–80, 83 S.Ct. 801, 9 L.Ed.2d 821 (1963); *Moore v. Ogilvie*, 394 U.S. 814, 819, 89 S.Ct. 1493, 23 L.Ed.2d 1 (1969)).

Although "there is no single, bright line to distinguish cases in which federal intervention is appropriate from those in which it is inappropriate," a viable election challenge:

> must go well beyond the ordinary dispute over the counting and marking of ballots .... Federal courts have properly intervened *when the attack was, broadly, upon the fairness of the official terms and procedures under which the election was conducted.* The federal courts were not asked to count and validate ballots and enter into the details of the administration of the election. Rather they were *confronted with an officially-sponsored election procedure which, in its basic aspect, was flawed.* Due process, representing a profound attitude of fairness between man and man, and more particularly between individual and government, is implicated in such a situation.

Duncan, 657 F.2d at 703 (internal citations omitted) (emphasis added).

As this Court recognized in its prior Order, the Supreme Court has cautioned that there are special considerations involved with federal intervention in impending elections:

> [O]nce a State's [election-related] scheme has been found to be unconstitutional, it would be the unusual case in which a court would be justified in not taking appropriate action to insure that no further elections are conducted under the invalid plan. However, under certain circumstances, such as where an impending election is imminent and a State's election machinery is already in progress, equitable considerations might justify a court in withholding the granting of immediately effective relief in a legislative apportionment case, even though the existing apportionment scheme was found invalid. In awarding or withholding immediate relief, a court is entitled to and should consider the proximity of a forthcoming election and the mechanics and complexities of state election laws, and should act and rely upon general equitable principles.

***57** *Reynolds*, 377 U.S. at 585, 84 S.Ct. 1362. "Confidence in the integrity of our electoral processes is essential to the functioning of our participatory democracy." *Purcell v. Gonzalez*, 549 U.S. 1, 4, 127 S.Ct. 5, 166 L.Ed.2d 1 (2006). Courts are "required to weigh, in addition to the harms attendant upon issuance or non-issuance of an injunction, considerations specific to election cases and its own institutional procedures." *Reynolds*, 377 U.S. at 585, 84 S.Ct. 1362. In *Purcell*, the Supreme Court explained that "[c]ourt orders affecting elections, especially conflicting orders, can themselves result in voter confusion and consequent incentive to remain away from the polls. As an election draws closer, that risk will increase." 549 U.S. at 4-5, 127 S.Ct. 5.

The current posture of this case presents an added wrinkle: this Court is reviewing Plaintiffs' challenge to the fraught GEMS/DRE system also in the context of the State Legislature's recent passage of new legislation requiring the Secretary of State to implement an entirely new voting system – to replace the existing DRE system, including the GEMS servers, DREs, and ExpressPoll units – prospectively "as soon as possible." O.C.G.A. § 21-2-300(a)(2). This is especially true considering the presumed deference to the State's interest in moving the state forward into a new voting system technology era. *See Anderson*, 460 U.S. at 788, 103 S.Ct. 1564 (recognizing that "as a practical matter, there must be a substantial regulation of elections if they are to be fair and honest and if some sort of order, rather than chaos, is to accompany the democratic processes"); *Duncan*, 657 F.2d at 702 ("The Constitution leaves to the states broad power to regulate the conduct of federal and state elections."). The adequacy of the newly chosen BMD election system is not before the Court at this time.

The Court disagrees with Defendants' assertions that Plaintiffs' requested relief is not feasible from either a timing or cost perspective, based on the scope of the relief at issue during an upcoming off-year election and the actual evidence presented by both parties. But the Court remains concerned, based upon the entirety of the record evidence, about the State's capacity to manage a transition to paper ballots for the 2019 elections while overseeing and undergoing a simultaneous transition to the newly enacted voting system during this time. And the Court is also concerned whether the State is prepared to fully implement the new system statewide in all 159 Georgia counties in time for the March 2020 presidential preference primary election as promised and provided for in the contract with its selected vendor Dominion Voting Systems. As addressed more below, the process thus far has already suffered from delays and modifications that are not insignificant in judging the Secretary of State's capacity to fulfill its statutory obligation of providing the uniform system of electronic ballot markers and ballot scanners for use in each county statewide "as soon as possible."

Although the contract specifies a final rollout date by Dominion that coincides with the March 24, 2020 presidential preference primary election date, the newly revised election code, O.C.G.A. § 21-2-300, does not impose a deadline for the Secretary of State's implementation of the new statewide voting system. *See* O.C.G.A. § 21-2-300(a)(2) ("*As soon as possible*, once such equipment is certified by the Secretary of State as safe and practicable for use, all federal, state, and county general primaries and general elections as well as special primaries and special elections in the State of Georgia shall be conducted with the use of scanning ballots marked by electronic ballot markers and tabulated by using ballot scanners for voting at the polls...")

(emphasis added). And as Mr. Beaver, the Secretary of State's CIO, acknowledged at the hearing – the implementation schedule "is tight." (Tr. Vol. I, Doc. 570 at 52.)

***58** All of these intensely practical factors in connection with the Secretary of State's rollout of the Legislature's new voting legislation (with a new voting mechanism) makes for a difficult brew. The public interest and balance of harms factors here – based on the unique factual posture of the case at this stage and the State Legislature's enactment of a new mode of voting to be implemented "as soon as possible" – weigh in favor of restraint in considering the full scope of relief sought by Plaintiffs for the 2019 election cycle. The Court must defer to the electoral machinery and processes chosen by the Legislature in HB 316 for prompt implementation, and thus has no basis at this juncture to order a hand-marked paper ballot scheme for the upcoming 2020 elections for which the Secretary of State is planning to conduct using the new BMD voting process. Given that limitation, Plaintiffs effectively seek implementation of hand-marked paper ballots for a single election cycle before the State transitions to an entirely new system that has been chosen to provide a voter verifiable paper record that in the future will be subject to some manner of auditing to evolve over the years to come according to the provisions of O.C.G.A. § 21-2-498. [95]

Of course, in light of all the problems plaguing the November 2018 election and the recognition by the State's lawmakers for the need to move away from DREs prior to the federal 2020 elections, the Secretary of State could have voluntarily chosen to abandon the DRE system and temporarily move to a paper ballot system for these off-year elections. (*See* PX 15, Doc. 565-8) (August 1, 2018 SOS Official Election Bulletin to County Election Officials and Registrars from Elections Division Director Chris Harvey stating, "There is a provision of Georgia law that allows the state to move to paper ballots in the event that the machines are inoperable or unsafe. If we ever reach a point where our office feels that these machines cannot be trusted to accurately deliver election results, we will invoke this statutory provision."). Despite this provision, the Secretary of State's officials have testified (twice) before this Court that the State does not have adequate resources or equipment or the necessary procedures in place to make the switch with a three-month lead time. They proclaimed the inability of the State to do so before a statewide election in November 2018, and they proclaim so again for off-year local and municipal elections in November 2019. (*See* Tr. Vol. 1, Doc. 570 at 47-48) (Merritt Beaver testifying that if the Court were to order the State to implement hand-marked paper ballots for elections in 2019, "I think we would have to make all efforts. That doesn't mean it would be successful. Without processes in place, we definitely would have issues. In fact, the issues may be major ... We would do it to the best of our ability. That doesn't mean it would be successful ... Somebody can ask us to do – something that it is not possible ..."). Not surprisingly, the State therefore has no backup plan for the DREs in the event of emergency or a systemic failure. More on that below.

The State's procurement of the new BMD system is in full swing with the goal of rolling out the system for 6 pilot counties in the November 2019 elections before moving forward with the statewide installment in all 159 counties. It is inevitable that requiring the State to pull needed resources from this large-scale implementation process to switch gears for the current election cycle would no doubt be highly disruptive as an administrative matter. It also might be a recipe for disaster given the State's lack of confidence and motivation in ensuring the success of such an endeavor. Although the Court views the continuation of the GEMS/DRE voting system as imposing a genuine threat to Plaintiffs' constitutionally protected voting rights that cannot be allowed to persist ad infinitum, it also confronts the reality that mandating change for one election cycle may well interfere with rollout of the Legislature's chosen statutory alternative voting scheme, enacted to address the inadequacies in the current system. The Court must weigh all requisite factors under the law prior to imposing significant injunctive relief.

***59** For all of these reasons, the Court finds it would be unwise to require the State to implement an intermediate hand-marked paper ballot system for the 2019 elections. But this particular weighing of the injunctive relief factors in the State Defendants' favor is confined to the unique circumstances of the 2019 off-cycle election before introduction of the newly mandated auditable BMD system. The analysis does not extend to all relief issues triggered by the Court's factual and legal findings as to the threatened constitutional deprivation and injuries at issue here. And most specifically, the Court's ruling prohibits any continued use of the GEMS/DRE system past the completion of the 2019 election cycle.

All that said, while the State Defendants have maintained that the BMD system will be rolled out in time for the federal Presidential Preference Primary elections in 2020 and that use of the DRE system in the 2019 elections is just a stopgap, the

Court has reason to doubt that. There are other dates and details regarding the implementation that have been a moving target, even putting aside the State's capacity issues manifested to date. In the April 9, 2019 status conference in this case, when State Defendants' argued that Plaintiffs' claims were mooted by the new legislation, counsel for the Secretary of State's Office represented to the court that: (i) the deadline for RFPs from vendors was April 23, 2019; (ii) the final valuation of the RFP would fall between June 18 through June 25, 2019; (iii) the State would finalize the contract terms with the chosen vendor through early July, 2019; (iv) the notice of award would be issued sometime in mid-July, around July 12 through July 19; and (v) by early August implementation would begin. These dates were based off and dependent on the scheduled close of the RFP process. (Tr., Doc. 363 at 6-8.)

The State delayed in issuing its initial Notice of Intent to Award until July 29, 2019. (*See* Doc. 552.) As no bid protests were received by the State, the Secretary of State issued its final Notice of Intent to Award on August 9, 2019. The Secretary of State also issued its Certification of the Dominion Voting Systems as meeting all applicable provisions of the Georgia Election Code and Rules of the Secretary of State on August 9, 2019.

Counsel also discussed at the April 19 conference with the Court the new statute's provision for the State to conduct "a pilot program for at least ten counties – but it could have more – to test – for testing purposes of the machines," so that actual elections will be run this year in 2019 on ballot-marking devices. (*Id.* at 8.) In an April 11, 2019 filing with the Court, the State Defendants further represented that "potential vendors must be able to initiate a ten-county pilot by August 2019." (Doc. 362 at 4.) But in July 2019, State Defendants informed the Court that the pilot program would only be launched in six counties, rather than ten. (*See* Docs. 556, 559.)

The State Defendants' counsel also represented that the State would conduct its pilot program in some major metropolitan areas, specifically "Fulton and Gwinnett" as part of the "Phase I" rollout and that "it looks like Fulton will have 200 ballot-marking devices for that phase."[96] (Tr., Doc. 363 at 9.) But as Richard Barron, the Director of the Fulton County Elections Office, testified in the 2019 hearing, Fulton County backed out of the pilot program based on perceived operational challenges. (Tr. Vol. II, Doc. 571 at 218.) And Gwinnett is no longer an ideal candidate for the pilot rollout because it has no scheduled elections in November 2019.

***60** And although the State told the Court in April 2019 that Fulton and Gwinnett Counties would be participating in the pilot program, only after the July hearing concluded did the State advise the Court that the pilot counties for the new voting system have not yet been definitively selected. (State Defs.' Resp. to Court Order, Doc. 559 at 2) ("As a practical matter, the selection of pilot counties depends on circumstances yet to occur, such as candidate qualifying (which ends on August 19, 2019 for November 2019 elections). In many local elections, only one candidate qualifies. If no election is held because the only candidate is unopposed, the county is useless for piloting a new voting system.") A "preliminary list" of counties to pilot the new voting system includes: Bacon, Bartow, Carroll, Catoosa, Charlton, Decatur, Evans[97], Lowndes, Paulding, and Treutlen.[98] (*Id.*)

Finally, the actual contract between the State and its selected vendor Dominion does not establish deadlines that permit "initiation" of the county pilot program in August 2019 as represented to the Court. The contract provides for receipt by the Secretary of State's Office and the 6 pilot counties of equipment during Phase I by September 13, 2019.

Given this slippage in just the initial stages of implementation of the new voting system and the State's significant scaling back of the planned pilot program for testing purposes, the Court has concerns about the State's ability to procure, test, and install the equipment for all 159 counties, implement an entirely new elections management, ballot building, and voter registration system, and perform the necessary training of local election officials in the schedule set by the State. As Plaintiffs have convincingly presented, the threat of election interference has only grown since they were here before the Court seeking relief one year ago in September 2018, while the State Defendants have only just begun to launch necessary steps to provide a more secure election. Given the State's demonstrated capacity limits in managing the issues that have arisen in connection with Georgia's elections systems to date and the evidence that the State itself has previously provided regarding the challenges of such a condensed time frame for a statewide rollout of a major change in voting methods,[99] the Court has real reason for concern regarding the State's

capacity for effectively handling the mammoth undertaking of starting from scratch and facilitating a rollout of the new voting system in 100 percent of the counties and precincts by the promised primary election deadline of March 24, 2020. The Court is further concerned whether the State has a backup plan other than the tainted DRE/GEMS system if its BMD system is not ready to launch in all counties statewide.

Based on its current plan of a progressively-phased rollout by county, the State must have a backup plan ready to be put in place because the risk inherent in the aggressive implementation schedule and the State's own demonstrated functionality issues may compromise the schedule. In opposing Plaintiff's motion, the State argued it did not wish to be put in the position of jeopardizing and testing the organizational capacity of its elections personnel to properly run an election because of any remedy required by the Court. The State must take sufficient and necessary action so that it does not put itself in that same position in the March 2020 Presidential Primary election and beyond – by leaving some portion of the State's voters in the position of being forced to use the current defective voting system as the default voting fallback. Continued use of the GEMS/DRE system past this 2019 cycle of elections is indefensible given the operational and constitutional issues at stake.

***61** With the scanning technology provided by Dominion under the State's contract and funds authorized in connection with HB 316, the State has available to it an acceptable default backup voting option. It is far more logical, efficient, and feasible to use the paper ballot scanning features of the State's newly adopted system as a compliment and default backup, rather than using the DRE/GEMS system, in the event problems with full implementation of the BMDs occur. And it is consistent with the ultimate objective and statutory scheme of the voter verifiable BMD system than the non-auditable, non-voter verifiable DRE system. To the extent there are administrative or fiscal issues arising from any need to acquire additional or different scanners from Dominion to enable a default option – if required – the Court notes that: (1) Dominion's RFP and contract documents clearly indicate its ready capacity to deliver additional scanners on a timely basis upon request; and (2) the Legislature authorized the expenditure of up to $150 million for the implementation of a new voting system – the Dominion contract came in at approximately $106 million. By contrast, if used as a fallback, the GEMS/DRE system would require a new round of ballot programming and building, separate from the new BMD ballot building – and it would require continued servicing and use of the DRE machines as well as coordination with the Secretary of State elections staff, just to start with.

Under the contract with Dominion, Georgia should have purchased the necessary paper ballots, optical scanners, and HAVA-compliant ballot marking devices for at least six counties for use in the November 2019 elections. The contract further requires that the State and Dominion will have completed training on the new procedures, systems, and equipment, and training protocols for the six pilot counties by the time of the November 2019 election.

Based on the legal posture of this case and constitutional relief issues at stake, the BMD rollout circumstances described above, the essential need for the Secretary of State's Office to plan for a default backup option in the event of incomplete rollout of the new BMD system for the March 2020 elections (other than use of the GEMS/DRE system in full or part), the State Defendants are **DIRECTED**:

(1) To refrain from the use of the GEMS/DRE system in conducting elections after 2019.

(2) To develop a default plan for use in the 2020 elections that addresses the contingency that the new BMD system enacted by the State Legislature may not be completely rolled out and ready for operation in time for the March 2020 Presidential Primary elections or in subsequent elections in 2020 and provide, as part of that contingency plan, for the use of hand-marked paper ballots for voting, in coordination with scanners and other equipment available through the State's contract with Dominion or amendment of such. To assist in the development of this contingency plan, the State Defendants shall identify a select number of counties or jurisdictions that agree to implement a pilot election in November 2019 using hand-marked paper ballots along with optical ballot scanners and voter-verifiable, auditable ballot records. [100] State resources (i.e., appropriate optical ballot scanners, voting booths, ballot supplies, and training materials, as needed) shall be made available for implementation of the pilot.

(3) File with this Court a copy of any proposed Rules as well as Final Rules adopted by the Georgia Board of Elections or the Office of the Secretary of State relating to protocols and provisions for the auditing of election results and ballots, as authorized or required under O.C.G.A. § 21-2-498 as amended, within two days of their issuance. *See also* O.C.G.A. §§ 50-13-4 and 50-13-7.

Plaintiffs additionally request injunctive relief relating to the voter registration database that the Defendants use as the foundation of the ExpressPoll system. Thus, as a matter of security of the voting process and ExpressPoll system tied to the casting of ballots, and to address on a narrowly tailored basis the voter database problems extensively identified here that present an imminent threat to voters' exercise of their right to vote, [101] the Court **DIRECTS**:

***62** 1. The State Defendants to develop a plan for implementation **NO LATER THAN JANUARY 3, 2020**, that addresses the procedures to be undertaken by election officials to address errors and discrepancies in the voter registration database that may cause eligible voters to (i) not appear as eligible voters in the electronic pollbooks, (ii) receive the wrong ballot, (iii) be assigned to the wrong precinct in the electronic pollbook, or (iv) be prevented from casting a regular ballot in their properly assigned precinct. A copy of the plan shall be provided to Plaintiffs' counsel.

2. The State Defendants should require all County Election Offices to furnish each precinct location with at least one printout of the voter registration list for that precinct.

3. The State Defendants should provide clear pre-election guidance to all County Election Offices regarding all polling officials' mandatory duty under law to provide voters the option of completing provisional ballots, including those who do not appear on the electronic voter registration database at a specific precinct or at all.

4. The State Defendants should continue in future elections to prominently post information concerning the casting of provisional ballots and voters' submission of additional information, including their registration status, and voters' capacity to check the status of their provisional ballot on the SOS website throughout the course of any state or federal elections.

5. The Secretary of State's Office should work with its consulting cybersecurity firm to conduct an in-depth review and formal assessment of the issues relating to exposure and accuracy of the voter registration database discussed here as well as those related issues that will migrate over to the State's database or its new vendor's handling of the EPoll voter database and function.

IV. CONCLUSION

The Plaintiffs' voting claims go to the heart of a functioning democracy. As the Court commented in its Order last year, "[a] wound or reasonably threatened wound to the integrity of a state's election system carries grave consequences beyond the results in any specific election, as it pierces citizens' confidence in the electoral system and the value of voting." *Curling*, 334 F. Supp. 3d at 1328. The reality and public significance of the wounds here should be evident – and were last year as well.

The long and twisting saga of Georgia's non-auditable DRE/GEMS voting system – running on software of almost two decades vintage with well-known flaws and vulnerabilities and limited cybersecurity – is finally headed towards its conclusion. The new Georgia electronic BMD voting system legislation adopted in 2019 was accompanied by a major funding appropriation. The legislation is an essential step forward out of the quagmire, even if just to terminate use of an antiquated vulnerable voting system, with funding for a replacement voting system and the initiation of some measure of future ballot audit protocols. The wisdom or legal conformity of the Secretary of State's selection of a new vendor's particular ballot system though is not the question now before the Court. [102]

***63** The past may here be prologue anew – it may be *"like déjà vu all over again."* [103] The Defendants have previously minimized, erased, or dodged the issues underlying this case. Thus, the Court has made sure that the past is recounted frankly in this Order, to ensure transparency for the future.

For the reasons discussed at length in this decision, the Court **GRANTS IN PART** and **DENIES IN PART** Plaintiffs' Motions for Preliminary Injunction [Docs. 387 and 419]. The Court **DENIES** Plaintiffs' request to enjoin the use of the GEMS/DRE system in the 2019 elections, but it **GRANTS** Plaintiffs' motion to the extent that the Court **PROHIBITS** any use of the GEMS/DRE system after 2019. The Court grants additional measures of relief, as described at the conclusion of Section V above. The Court specifically grants narrowly tailored relief measures to ensure that the GEMS/DRE system is not resorted to as a stopgap default system in the event the Secretary of State and its contractor are unable to fully and properly rollout the new BMD system in time for the 2020 Presidential Preference Primary or any of the ensuing elections. And it requires that the State Defendants promptly file with the Court all proposed and final audit requirements that the State Elections Board and Secretary of State's Office considers or approves in connection with elections to be held in 2020 or thereafter. Finally, the Court views the significant voter registration database and related ExpressPoll deficiencies and vulnerabilities demonstrated in this case as a major concern both relative to burdening or depriving voters' ability to actually cast ballots. The Court therefore requires the State Defendants to develop procedures and take other actions to address the significant deficiencies in the voter registration database and the implementation of the ExpressPoll system.

IT IS SO ORDERED this 15th day of August, 2019.

All Citations

--- F.Supp.3d ----, 2019 WL 3822123, 104 Fed.R.Serv.3d 537

Footnotes

1 Plaintiffs forcefully opposed any stay of the proceedings and immediately sought a status conference to discuss an expedited schedule to move the case forward in time to address future elections. Despite having found the State Defendant's immunity and standing arguments meritless and expressing its strong concerns regarding the need for the State to move forward to address election remedial issues, the Court nonetheless reluctantly granted the stay request pending appeal to the Eleventh Circuit due to the exceptionally high legal standard for showing of frivolousness required in this context. On an expedited appeal, the Eleventh Circuit denied and dismissed the State Defendants' appeal of the Court's jurisdictional rulings on immunity and standing in a decision deemed final on March 8, 2019.

2 The two sets of Plaintiffs in this case are represented by separate counsel and have sought overlapping but somewhat different equitable relief. Donna Curling, Donna Price, and Jeffrey Schoenberg are referred to as the "Curling Plaintiffs." The Coalition for Good Governance ("CGG"), Laura Digges, William Digges III, Ricardo Davis, and Megan Missett are referred to as the "Coalition Plaintiffs." *See* Section IV *infra* regarding the overlapping but distinct relief measures requested by the two groups of Plaintiffs.

3 For the sake of efficiency, the Court refrains from repeating the full range of factual findings and assessments of the evidence already set forth at length in its September 17, 2018 Order and that the Court finds still applicable.

4 CES at KSU functioned as a contractor and agent of the Secretary of State's Office in performing critical election management and data management duties for both State and county election processes. CES managed the State's GEMS server, which stores state and county election and voter data. CES also furnished data to create the lists of voters for electronic poll books used in each election, performed all ballot building processes, provided support for all jurisdictions in the election process and in support of DREs, and overall played an essential role in the operation of elections. The Agreement between the Secretary of State and Board of Regents through KSU makes plain that at all times the CES functioned as the agent of the SOS in performing and managing these critical functions on behalf of the SOS and the SOS Elections Division. (Doc. 258-1.)

5 On July 7, 2017, four days after this lawsuit was originally filed in Fulton Superior Court, all data on the hard drives of the University's CES server on "elections.kennesaw.edu" were wiped or destroyed. And on August 9, 2017, the day after this lawsuit was removed to federal court by Defendants, all data on the hard drives of a secondary server which contained similar data was also wiped or destroyed. *Curling*, 334 F. Supp. 3d at 1310.

6 The Secretary of State's Office absorbed CES on January 1, 2018. CES's Director, Michael Barnes, at that time also transferred back to the State and continues to serve as the Director of CES.

7 *See United States of America v. Viktor Borisovich Netyksho et al.*, Criminal No. 1:18-cr-215 ¶¶ 69, 75, 2018 WL 3407381 (D.D.C., July 13, 2018).

8 Georgia Act No. 24, Georgia House Bill 316, amending Chapter 2 of Title 21 of the Official Code of Georgia Annotated.

9 *See* O.C.G.A. § 21-2-300. The state additionally authorized up to $150 million for the contract with a private vendor, to be selected, for purchase of election equipment, software, and services in connection with the new voting equipment and electronic pollbook equipment and supporting software for the electronic voter check-in and verification system at the polls.

10 The State's contract with Dominion calls for in-precinct scanner/tabulators for the "paper" ballots generated by the Ballot Marking Devices ("BMDs"). The contract also calls for rapid full ballot image/ballot counting scanners for absentee and provisional ballots that are handled in the board of elections office in each county. The printer attached to each BMD used for in-person voting on which the elector electronically marks her vote produces a printed list of the candidates the elector has voted for as opposed to an image of the entire completed ballot as it actually appears on the BMD device screen or if printed on an absentee ballot. The ballot scanner tabulates the selections from each ballot based on the bar code imprinted on the paper printout scanned as opposed to the listing of candidates. The Plaintiffs point out that no elector can visually review and confirm whether the bar code accurately conveys her votes actually cast, as filled out on the BMD screen or appearing on the printout. In other words, a voter cannot verify upon inspection what the bar code on the ballot signifies, *i.e.*, what vote it actually is recording. The State appears to rely on its assessment of the reliability of the equipment software as a whole, the scanner, and the provision of auditing to address this concern. The parties also appear to dispute whether the bar code feature of the new ballot system is consistent with the requirements of the legislation. The State's own expert, Dr. Michael Shamos is not a fan of the type of ballot marking devices chosen by Georgia for its new $106 million election system that rely on a computer-generated barcode to tabulate the votes, the accuracy of which cannot be verified by the voter. (Shamos Dep. at 56-57.) He agrees that the more reliable approach is the use of a BMD that produces a paper record of the vote tabulation readable by the human voter. (*Id.* at 57.) In any event, this dispute as to the reliability of the bar code voting modality as a transparent, reliable mechanism or it's conformity with state law is one not encompassed in the preliminary injunction motions before this Court.

11 The Fulton County Defendants include the Director and members of the Fulton County Board of Registration and Elections (Richard Barron, Mary Carole Cooney, Vernetta Nuriddin, David J. Burge, Stan Matarazzo, and Aaron Johnson) in their official capacities.

12 The plaintiffs in *Fair Fight Action* asserted numerous challenges including that "Georgia's election system, including its voter registration data and voting machines, lacks adequate data security, imposing a severe burden on Georgia voters' right to vote." (Order, Doc. 68 at 33.)

13 The State Defendants argued in an April 11, 2019 filing that "[i]f counties are unable to use their existing election system to conduct municipal elections, they may choose not to enter into contractual agreements with the affected municipalities, leaving the municipalities with limited time to implement and fund an interim election system." (Doc. 362 at 10.) This is pure speculation and unsupported by any record evidence. The argument also ignores the reality (based on the information provided to the State Defendants by the counties and municipalities for the 386 scheduled elections thus far) that these intra-governmental agreements have already been executed for the 2019 elections. Any existing contracts would have to be breached for the State Defendants' argument to work.

14 The State Defendants are aware of at least four (4) municipalities that own their own DREs which will be used in the upcoming November 2019 municipal elections: Riverdale, Chickamauga, College Park, and Eatonton. (Doc. 537 at 2.)

15 Elections Systems & Software ("ES & S") is Georgia's elections equipment vendor for the current DRE/GEMS system.

16 In response to a request by the Court for an updated list of scheduled elections in 2019, State Defendants offered the Declaration of Melisa Arnold, the City Clerk and Elections Superintendent for the City of Snellville in Gwinnett County and the Declaration of James E. Elliott, Jr., the former City Attorney for Warner Robins. (*See* Doc. 537-1; 537-2.) The City of Snellville does not contract with Gwinnett County to conduct its municipal elections. (Doc. 537-1 ¶ 4.) Rather, Snellville conducts elections using hand-marked paper ballots tabulated by an optical scan machine at a single precinct location. (*Id.* ¶¶ 4, 14.) The City of Snellville owns two (2) AccuVote ES 2000 optical scan machines for tabulating the paper ballots for use by voters at the precinct for scanning of their ballots. (*Id.* ¶¶ 4, 6.) Ms. Arnold opines in her "experience in conducting elections with paper ballots" that she has "serious concerns regarding the implementation of a new method to conduct elections at this time," based on expenses associated with procuring new equipment, certifying equipment, training poll workers, and educating voters. (*Id.* ¶ 22.) The Court struggles to see the relevance of Ms. Arnold's opinion, as Snellville currently uses the exact paper ballot voting method Plaintiffs seek in this case. Mr. Elliott is not an election superintendent in Warner Robins. Rather, in his former role as City Attorney, Mr. Elliott "advise[d] the City Officials on all legal matters as General Counsel, including zoning, licensing, and elections issues." (Doc. 537-2 ¶ 3.) Mr. Elliott does not offer any actual opinion on the burden or feasibility of a change by Warner Robins from DREs to paper ballots. (*See id.*) Instead, the purpose of his declaration appears to be to offer this Court his legal opinions on the interpretation of Georgia's election code. (*See id.* ¶ 11 ("Based

on the framework of the law surrounding municipal elections, it is unclear how various municipalities may be affected by the relief requested by Plaintiffs in this case.").

17 *See* Advisory Committee Notes, Fed. R. Civ. P. 19 ("Even if the court is mistaken in its decision to proceed in the absence of an interested person, it does not by that token deprive itself of the power to adjudicate as between the parties already before it through proper service of process. But the court can make a legally binding adjudication only between the parties actually joined in the action. It is true that an adjudication between the parties before the court may on occasion adversely affect the absent person as a practical matter, or leave a party exposed to a later inconsistent recovery by the absent person. These are factors which should be considered in deciding whether the action should proceed, or should rather be dismissed; but they do not themselves negate the court's power to adjudicate as between the parties who have been joined.")

18 Significantly, HAVA also required every state to implement a single centralized, computerized, statewide voter registration list containing the name and registration information of every legally registered voter in the State. 52 U.S.C. § 21083(a)(1)(A).

19 Dr. Halderman's extensive qualifications as Professor of Computer Science and Engineering and Director of the University of Michigan Center for Computer Security and Society have been previously described.

20 Mr. Hursti has performed several cybersecurity examinations of electronic voting machines of the type used in Georgia.

21 As Hursti's report explains in greater detail: "Unlike the desktop versions of Windows, the embedded versions of Windows CE 3.x and 4.x versions used in the Diebold system (which are both noncurrent versions) have very limited security features against a user with access below the application level. Because of the lesser security available in Windows CE, access to the standard Windows Explorer application grants users access to replace and modify files almost without restriction. This enables a hostile attacker to severely alter the system functionality and/or add new software (and hidden processes) to the system. In addition to altering individual files, the TSx and TS6 systems also present opportunities to change the Operating System itself. This provides possibilities for hiding the attack and/or altering the application's behavior without any changes to the application itself. A major contributor to this is the ability to change the Operating System functions and libraries any application software relies on at a deep level." (*Id.* at 3-4.)

22 A related software program, maintained and licensed by PCC (a different company than ES & S that licenses the GEMS / DRE software), is used to create the ExpressPoll pollbooks providing confidential voter identification information by precinct. Poll workers access this data by computer to verify voter registration and to create the DRE Voter Access Card, which activates the specific electronic ballot on the DRE machine that should be linked to the voter's address and precinct.

23 Theresa Payton of Fortalice Solutions, retained by the State to evaluate the security of the Secretary of State's general computer network system, testified at the 2019 hearing that while software patches are available for the Windows XP operating system, she "wouldn't want to run [her] stuff on it." (Tr., Doc. 570 at 275.)

24 Until the November 2018 election, the SOS allowed county elections offices to transmit their election night results by modem to the state election night server. According to the Election Supervisor for Morgan County, called as a witness by Defendants, the current established state protocol she follows on election night for transmission of County returns instead of the modem transmission is to (1) copy on a flash drive the GEMS election results datafile; (2) take that drive to her internet connected computer; and (3) upload the GEMS vote tabulation results to the Election Night Reporting website run via PCC for the SOS. (Tr., Doc. 571 at 326.) The Georgia State Patrol transports the final CD containing the GEMS database election results from each county back to the SOS some days later, after the County Board of Elections has certified the vote totals.

25 But he admitted he had no knowledge regarding the security of the software on which the GEMS server operates or "what levels of security they have surrounding that entire system." (*Id.* at 227.)

26 Merritt Beaver, the Chief Information Officer at the Secretary of State's Office testified at the 2019 hearing that there is no endpoint protection on the GEMS server because they consider the server air gapped. (Tr., Doc. 570 at 61-62.)

27 Mr. Barnes often refers to the private computer housing the GEMS server as "air gapped." However, as Dr. Halderman and Dr. Shamos both testified – the actual process used by the Secretary of State's Office does not constitute an "air gapped" system as explained below. The Court will therefore refer to "private" as not being directly connected to the internet.

28 Two of these individuals previously worked for Barnes at CES and the third worked for Cobb County. (Tr. Vol. 1, Doc. 570 at 85.) Barnes was not aware of whether these individuals were employees of ES & S or independent contractors.

29 The pubic internet-computer screens for standard known malware.

30 There was no means of detection of this as the "malware modified all of the vote records, audit logs, and protective counters stored by the machine, so that even careful forensic examination of the files would find nothing amiss." (Halderman Decl. ¶ 19, Doc. 260-2.)

31 Dr. DeMillo, who also testified at the 2018 hearing, is the Chair of Computer Science at Georgia Tech and Director of the Georgia Tech Center for Information Security, having previously served as the Dean of the College of Computing at Georgia Tech and Chief Technology Officer for Hewlett-Packard. (Doc. 548 at 74.) Dr. DeMillo has conducted research and taught courses relating to voting system and election security since 2002. He helped write guidelines for using electronic voting machines for use by the Carter Center. He also serves on the advisory boards of Verified Voting and the Open Source Election Technology Institute. (*Id.*) Dr. DeMillo is

familiar with Georgia's Diebold DRE voting system, its design, the body of academic literature on the system from the last ten years, and its operation as it is deployed in the polling places in Georgia. He is likewise familiar with Georgia's testing procedures conducted prior to machine deployment at the polling places. Dr. DeMillo owns both the Diebold TSx and TS voting machines which he has examined and used to conduct certain experiments related to DRE system security. (*Id.* at 75.) In his November 21, 2018 Declaration, Dr. Richard DeMillo discussed his observations of DRE voting machine and electronic pollbook malfunctions while he served as a statewide pollwatcher during the November 6, 2018 election. (Doc. 548 at 77.) On the afternoon of November 6, 2018, Dr. DeMillo conferred with Harri Hursti (the nationally recognized Diebold voting systems expert that discovered the severely compromised nature of the AccuVote TSX software in 2006 previously mentioned by the Court above) and cyber security researcher Logan Lamb. Hursti and Lamb had just completed a review of technical information at the Anistown voting precinct in Gwinnett County where four-hour voting delays were being attributed to malfunctioning ExpressPollbooks. (*Id.*)

32 *See, e.g.*, Eric A. Fischer, Cong. Research Serv., RL32139, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues* (2003) ("there appears to be an emerging consensus that in general, current DREs do not adhere sufficiently to currently accepted security principles for computer systems"); David L. Dill, Bruce Schneier & Barbara Simons, Voting and Technology: *Who Gets to Count Your Vote?*, 46 Communications of the ACM 29 (Aug. 2003) (explaining, "[a] computer can easily display one set of votes on the screen for confirmation by the voter while recording entirely different votes in electronic memory, either because of a programming error or a malicious design"); Tadayoshi Kohno, et al., *Analysis of an Electronic Voting System, 2004 IEEE Symposium on Security and Privacy* 27 (2004) (discussing researchers' findings that DRE software is significantly flawed after the source code for a DRE voting machine was accidentally posted online); Joseph A. Calandrino, et al., *Source Code Review of the Diebold Voting System* 10, Univ. of Cal. (July 20, 2007) (finding the systems of California's DREs were susceptible to viruses and malicious software, i.e. "malware"); Ariel J. Feldman, J. Alex Halderman, & Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine, USENIX/ACCURATE Electronic Voting Technology Workshop* (2007) ("[A]nyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes as little as one minute.").

33 The NASEM (or NAS, for short) was established by Congress in 1863 to provide independent scientific and technical advice to the Government. The NAS study committee was charged with: 1) documenting the current state of technology, standards and resources for voting technologies; 2) examining the challenges arising out of the 2016 federal election; 3) evaluating advances in current and upcoming technology that can improve voting; and 4) providing recommendations to make voting easier, accessible, reliable, and verifiable. (Doc. 285-1, Ex. 1 at 4.) The committee members, including Dr. Appel met over 16 months and heard testimony from experts and election administrators. After the study passed a separate independent peer review, it was released by the National Academies of Sciences in September 2018 under the title *Securing the Vote: Protecting American Democracy.* As noted by Dr. DeMillo in his supplemental declaration in 2018, "a consensus report of the NAS ... represents the highest authority that the U.S. Government can rely upon when it seeks to be advised on matters of science, technology and engineering." (Doc. 285-1 ¶¶ 8, 9.)

34 Report of the Select Committee on Intelligence on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Vol. 1: Russian Efforts Against Election Infrastructure with Additional Views, 116th Cong., 1st Session (2019) (*partially redacted*) ("SSCI Report"). The Senate Select Committee on Intelligence, which was released to the public on July 25, 2019, "sought to determine the extent of Russian activities, identify the response of the U.S. Government at the state, local, and federal level to the threat, and make recommendations on how to better prepare for such threats in the future." (*Id.* at 3.) The redacted SSCI Report was presented at the July 26th hearing marked as Defendant's Exhibit 3, but Defendants did not move for its admission into evidence.

35 This "assumes that the scanner itself does not maintain an image of the ballot. It counts the ballot, but it doesn't keep a copy of the ballot," unlike modern scanners used in connection with the hand-marked paper ballot election system. (Shamos Dep. at 27.)

36 Dr. Shamos admitted in his deposition that it is also true that anytime a programmable computer voting machine is used to count a vote, the count can be modified and a "miscalibrated DRE will not capture a vote accurately." (Shamos Dep. at 34-35.)

37 In his deposition, Dr. Shamos testified that he believes that Georgia uses the AccuVote OS model that scans ballots using infrared light, as opposed to the model that makes an optical scanned image of the ballots that is stored on the memory cards. (Shamos Dep. at 195-96.) The record in this case suggests that the State purchased and uses both models of the AccuVote OS, the older model that uses infrared scanning technology purchased when the State formerly used paper ballots in 2000 and with the initial rollout of the DRE system in 2001 to 2002, and newer models using optical scan technology obtained later by the State for incorporation into the system for use with absentee and provisional ballots.

38 However, election administrators Russell Bridges from Chatham County and Lynn Ledford from Gwinnett County testified at the preliminary injunction hearing in this case that, when scanners used at the precinct level are either unable to accurately read a ballot or detect overvotes, voters are given the opportunity to complete a new ballot. When such errors are registered on a central count scanner, the elections officials will prepare hand-duplicate ballots based off of the original ballot completed by the voter. (Tr., Vol. 2, Doc. 571 at 262-263, 309.)

39 According to Dr. Shamos, this assumes the voter's intent can be properly interpreted under Georgia SEB Rule 183-1-15-.02, *i.e.*, the voter must follow the instructions and properly mark the ballot for her markings to constitute a vote.

40 The experts disagree on the type of optical scan systems used in Georgia. Dr. Shamos believes that Georgia's scanners do not store an optical scan copy of the ballot image. It is Dr. Halderman's understanding of the information he has knowledge of that Georgia does use an AccuVote OS model that stores an actual image of each ballot scanned. Either way, O.C.G.A. § 21-2-300, enacted April 2, 2019, requires the State to furnish new ballot scanners for use in each county as soon as possible. As Dr. Appel noted in his Declaration, modern precinct-count optical scan machines scan a high-resolution image of the entire ballot page and the memory image in the precinct-count optical scanner "can provide important forensic evidence if it is suspected that the paper ballots have been tampered with." (Appel Decl. ¶ 2, Doc. 510-2; 524-2.)

41 Mr. Hursti is a computer programmer and noted data security expert who has performed several cybersecurity examinations of electronic voting machines used in Georgia.

42 Dr. Shamos served as an electronic voting system certification examiner for Pennsylvania from 1980 to 1996. From 2004 to 2017, he served as a consultant to the Secretary of the Commonwealth of Pennsylvania on electronic voting matters.

43 And while noting that paper ballots are not without challenges, the NAS report concluded that "[w]ell designed, voter-marked paper ballots are the standard for usability." (*Id.* at 79.)

44 Dr. Appel agrees that Georgia does not do effective parallel testing. (Appel Decl. ¶ 30, Doc. 510-2; 524-2) (identifying his review of August 1, 2018 letter from Chris Harvey to County Commissioners describing an extremely ad-hoc and lightweight regime for parallel testing used by Georgia in 2018). According to Dr. Appel, "[p]arallel testing would be an extremely labor-intensive and impractical means of detecting DRE fraud, if it were ever done as thoroughly as would be necessary to be reliable. There is no evidence that parallel testing has ever been done, in any state, at a large enough scale to reliably assure the absence of DRE hacking." (Appel Decl. ¶ 29, Doc. 510-2; 524-2.)

45 William Shakespeare, *The Tempest*, Act 2, Scene 1.

46 Doc. 472-10 at 9; 472-4 at 2. *See also*, https://news.kennesaw.edu/stories/2006/Center-for-Election-Systems-provides-national-leadership-on-voting-issues.ph.

47 Mr. Barnes's educational background is in public administration. He has no formal training or expertise in computer science or cybersecurity. However, he previously served as Assistant Director of Elections for the Georgia Secretary of State prior to his move to the CES/KSU in 2005 and directed the State of Georgia's operational transfer to the GEMS / DRE system. (Doc. 472-4 at 1.)

48 Mr. Lamb's affidavit describes the simple scripts that he used to access multiple megabytes of sensitive voter and GEMS data and structural information, that was either publicly accessible or poorly encrypted. He also noted in his email that the Kennesaw server was using Drupal software that is subject to "drupaggedon" malware for which there was a 2014 public advisory, alerting users that an attacker with this malware could now or could previously have created, modified, or deleted files on web servers without detection. (Doc. 258-1 at 128-133.)

49 Barnes's first instinct after receiving this news (which he soon retracted on August 29, 2016) was to direct that Mr. Lamb and his cybersecurity firm be placed on a blacklist of addresses. (Doc. 258-1 at 368.)

50 For instance, Mr. Barnes's deposition testimony and Open Records email documentation furnished in connection with Mr. Lamb's affidavit indicates that CES/KSU staff, after notification of Lamb's concern regarding the scope of data exposed in the absence of an essential Drupal software patch, only then sought to apply the patch. As one of the CES website managers wrote, "Unfortunately, until today, the CES website was built on Drupal before either of us were employed here and we have spent the last several years simply maintaining it in the order it had been working previously. Obviously, this has become untenable in the current atmosphere and Jason and I must learn more to get the security of the website under control.... " And after just then installing the patch, the CES staff member comments, "it seems the file tree had been available to anonymous users.... We are currently [ ] having trouble patching the ability for anonymous users to access individual files." (Doc. 258-1 at 246.) Mr. Barnes was copied on this and almost all other communications that occurred after Mr. Lamb's proactive efforts to provide alerts to CES / KSU leadership staff in August 2016 and the March 2017 alerts to CES/KSU of the profound and continuing data exposure and breach via the CES/KSU website. Similarly, when the Elections and backup Unico server were finally scanned in mid-October 2016, the Associate Executive Director of KSU Information Security emailed Steven Dean, the Technical Director for CES/KSU about the scan identifying one "critical vulnerability" (invalid logins permitted) on the Unicoi server as well as plain text logins that provide "opportunity for malicious users." He also noted that the Elections server was still showing use of an outdated version of server-side software (PHP) (used to create dynamic webpages that interact with databases) and that "this might be the reason 40+ critical vulnerabilities are being identified as related to PHP." (Doc. 258-1 at 229-30.)

51 The Court notes, though, that the SOS subsequently purchased new servers for operation of the GEMS system.

52 In stating this, the Court observes that it has carefully reviewed the parties' briefs and additional attached evidence as to spoliation issues. The notion, argued by Defendants, that Lamb's exposure of the software flaws and data system exposure was not front and

center in the original state lawsuit (later removed to this Court) is far-fetched. (*See* Doc. 1-2, ¶¶ 1-36, 93-95, 98) (recounting the entire set of episodes involving the software defects and data breach and vulnerabilities identified by Lamb and his colleagues and relying on such in Plaintiffs' claims that Defendants had run the congressional election on an insecure, unsafe, and compromised election data system, inclusive of defective DRE voting machines); *see also*, Count II claim pursuant to 42 U.S.C. § 1983.) Service of the July 3, 2017 lawsuit was provided prior to the server destruction and news of the filing of the suit appeared soon after its filing.

53 The Coalition Plaintiffs did not file a spoliation sanctions motion but instead requested that the Court view the evidence through the lens of spoliation legal doctrine and presumptions in a hearing brief filed on July 25, 2019. And in that connection, the Coalition Plaintiffs ask the Court also to consider other evidence regarding Defendants' alleged mis-handling and failure to preserve DRE machines and memory cards that were subject to litigation holds and preservation obligations. The Court was actively involved in assisting the parties in addressing voting equipment preservation agreements that both preserved voting equipment evidence for later inspection and trial and allowed flexible arrangements to assure that no county would lack sufficient equipment for running elections. Given the extended period when discovery in this case was stayed due to Defendants' motions to dismiss and appeal and that Plaintiffs only filed their spoliation brief during the most recent injunction hearing, the Court will not endeavor to parse out at this point all that may well have gone wrong in preservation of the DRE machines and cards.

54 The Court cannot fathom why Defendants' prior counsel did not proceed with their representation to Plaintiffs' counsel in their October 26, 2018 notice of intent to subpoena the FBI's CES/KSU server images for evidentiary preservation purposes. Fortunately, despite the notice's statement that the FBI would otherwise destroy the image because the FBI's KSU investigation was now closed, that apparently has now turned out to be incorrect. The FBI has now indicated the server images remain available and will make arrangements for their production. What data was left on the servers imaged, however, remains a question.

55 As noted earlier, HAVA requires every state to implement a single centralized, computerized, statewide voter registration list containing the name and registration information of every legally registered voter in the State. 52 U.S.C. § 21083(a)(1)(A). Georgia contracted for years with PCC Technology, Inc. (PCC) to handle the function of maintaining the voter registration system of record and house the voter database. PCC owns and operates the "ElectioNet" or "eNet" data suite of software system for operation of the voter registration data system. When a citizen in Georgia registers to vote and submits a voter registration application, county election officials input the information from the application into eNet. The following voter information is included in eNet: residence information, biographical information, personal identifying information (driver's license and social security numbers), districting information (House, Senate, Congress), and voting history. Confidential voter identification data from eNet is fed directly into the "ExpressPoll" electronic pollbooks. Poll workers access this pollbook data by computer to verify voter registration on election day (and to create the DRE Voter Access Card that activates the specific electronic ballot on the DRE machine that should be linked to the voter's address). The Secretary of State also operates and maintains a public website ("My Voter Page" or "MVP"), that operates with PCC software. Voters can use the webpage to look up their publicly available voter information, verify their voter registration status, and also enter data modifying their address.

56 Fortalice partnered with Cloudburst Security in performing security evaluations and the first two evaluations, issued in October 2017 and February 2018, were done under the name "Cloudburst Security team." (PX 1, (Docs. 510-5, 510-7.) The third and final report appears to have been issued solely under the name of Fortalice Solutions. (PX 3, Doc. 510-6.)

57 The Court notes, though, that the State recently advised the Court that effective July 1, 2019, it had modified its contract with its long-term vendor PCC that owns the license for the statewide voter registration eNet software. PCC hosted and managed Georgia's voter registration databases until July 1, 2019 when the State modified its contract to take over that function. PCC continues to own the license for the voter registration eNet software applications and remains under contract with the State for maintenance and support of the software applications. The State has thus far provided limited information to the Court regarding how it will perform this function other than that it is taking over hosting the data base. (Tr. Vol. 1, Doc. 570 at 70-71.) The Court notes, though, that the SOS's new contract with Dominion Voting Systems dated July 29, 2019, provides for Dominion's provision and billing for electronic pollbook hardware and software and the State Defendants' July 30, 2019 filing clearly indicates that Dominion will be managing the electronic pollbook function. (¶ 10.1.7; Doc. 556.)

58 As to the scope and limitations of the July 1, 2019 transfer, *see* testimony of SOS Chief Information Officer Merritt Beaver, Tr. Vol. 1, Doc. 570 at pp. 69-70.

59 Fortalice assessed the significance of these risks in connection with the National Institute of Standards and Technology Cybersecurity Framework ("NIST Framework").

60 As discussed later in this Order, according to Fortalice's November 2018 report, 3 of the 22 risks had been remediated as of November 2018, when the last statewide election was held.

61 The 2017 Fortalice report further found that Fortalice/Cloudburst was able to identify instances of voter registration data hosted on file shares available to all SOS domain users.

62 In his 2019 hearing testimony, Mr. Beaver endeavored to parse the significance of the Fortalice finding, by pointing out that the immediate penetration testing was conducted on one of the two SOS data centers – the one that holds the corporations' database, professional licensing database, and SOS website but not the elections system and voter registration system. (Tr. Vol. 1, Doc. 580 at pp. 44-45.) However, Ms. Payton and the Fortalice/Cloudburst Reports clearly did not limit the significance or scope of the Fortalice/Cloudburst penetration findings, i.e., that their penetration efforts yielded expansive access to the network security system, administrator rights and control of the network domain, and access to the enterprise architecture and system configurations.

63 Plaintiffs' cybersecurity expert witness, Dr. Alex Halderman clearly discussed at the July 26, 2019 hearing once again how penetration in one part of the state or county voting system can well result in the spread of malware to other parts of the system, whether in the CES computers, or the county DRE voting equipment and voting cards. (Tr. Vol. 2, Doc. 571 at pp. 92-98.) This testimony is consistent with that of a host of state and national studies as well as other expert affidavits that Plaintiffs have introduced or referenced in the record and the opinion of State Defendants' expert Dr. Shamos. (*See also*, Doc. 437-1) (extensive discussion of such in Brief of the Electronic Privacy Information Center as Amicus Curiae in Support of Plaintiffs' Position at Trial.)

64 A variation of this occurs when a voter presents to vote in a less than countywide election but is not shown as eligible to cast a vote in a particular election or precinct and the voter may then be incorrectly advised that she is not eligible to vote at all, as opposed to being eligible to cast a vote in that precinct using a provisional ballot. (PX 16, Doc. 565-16 at 4.)

65 In his August 3, 2018 declaration, Mr. Lamb additionally makes clear the implications of the loose accessibility of passwords for election day supervisors. “Supervisor passwords control the administration of the DRE voting machines in the polling place including opening and closing of the voting machines as well as making administrative corrections when problems are encountered.” (Doc. 258-1 at 130.) He also notes that the ExpressPoll units' files can be modified when voters are checked in to vote, so as to change the voter's assigned “ballot style” (i.e. ballots differ depending on the electoral races listed) and impact whether the voter is approved for voting at the specified polling place. (*Id.* at 130-131.)

66 To assure SOS system security, the Court here will not discuss in greater detail Fortalice's methods or findings in connection with this 2018 penetration testing.

67 The declaration was filed as a sealed document. As the declaration is directly germane to this case and the attempted hack addressed in it was discussed in open testimony in this Court, the Court perceives upon review that good cause does not support maintaining the sealed status of the declaration. The Court has therefore ordered that the declaration be unsealed and takes notice of the content of the declaration.

68 The Court surmises that this or another similar incident or the CES/KSU gaping exposure of voter in 2016-2017 – is what Mr. Beaver referred to in his testimony at the July 25, 2019 hearing.

69 The Court confirmed this change of address input option by accessing the MVP website, https://www.mvp.sos.ga.gov/MVP/mvp.dothe MVP Login and choosing the option of “change voter information.” (August 8, 2019). In viewing the MVP website, the Court also viewed the MVP tab “elected officials” available for voters. When the Court attempted to view this page with a Mozilla Firefox browser, the Court received this blocking message: “Your connection is not secure. The owner of www.sos.georgia.gov has configured this website improperly. To protect your information from being stolen, Firefox has not connected to the website.” https://www.mvp.sos.ga.gov/elections.statewide.htm. The Court then used a different computer and browser and received a similar but differently worded insecurity message.

70 The State's contract with Dominion provides that “Dominion's Democracy Suite Election Management System shall have the capability of importing election data from the State of Georgia's current database to generate ballot layout used to conduct an election.” (Contract, Ex. B, § 10.8 at p. 61.) According to the State's filing in response to this Court's inquiry, “the database referred to in Section 10.8 is the voter registration database,” which “creates a flat, delimited text export file that contains no executable code and includes precinct and ballot combo information for import into [Dominion's] EMS.” (Doc. 556 at 3.) The State's RFP provides that the vendor's new EPoll Data Management System must have the following capabilities: (i) being “[u]sed to combine voter registration and election ballot data into an election-specific elector's list that power the electronic poll book (EPoll) and provides each voter with the properly assigned ballot style;” and (ii) “[a]ccept[ing] imports of voter registration data from eNet on removable memory devices for the purposes of building an elector's list for any given election. The data transferred from eNet includes but is not limited to: voter name, voter address, driver's license number, voter registration ID, voter status, assigned precinct, assigned district combination value, assigned polling place, polling place address, [and] absentee status.” (eRFP, Attachment M at 1.) Thus, under the State's proposal and contract provisions, there is a real potential of importing erroneous or corrupted data from the existing eNet database into the new EPoll Data Management System.

71 Twenty-seven of these affidavits are from voters describing various problems with absentee ballots. The Court considers this evidence only in the context of Defendants' assertions that voters who lack confidence in the DREs have the option of voting by absentee paper ballots along with recent security bulletins issued by the Department of Homeland Security Office of Intelligence & Analysis in September and October 2018 warning states, including Georgia specifically, of foreign threats to elections systems and specifically

threats to absentee ballot systems. *See* September 5, 2018 DHS bulletin, Doc. 471-1 at 34 (warning states to be vigilant about "[a]ttempts to access, alter, or destroy systems used to ... process requests for absentee ballots...." and "[a]ttempts to access, hack, alter, or disrupt infrastructure to receive and process absentee ballots through tabulation centers, web portals, e-mail, or fax machines; attempts to interfere with votes sent through the U.S. Postal Service"); October 2, 2018 bulletin "A Georgia Perspective on Threats to the 2018 U.S. Elections," Doc. 471-1 at 37 (warning DHS I & A "assess that foreign governments may engage in cyber operations targeting election infrastructure ... DHS I & A is particularly concerned about the potential for the following activities related to the 2018 U.S. election: ... Attempts to hack, alter or disrupt infrastructure used to process absentee ballots or attempts to interfere with votes sent through the US Postal Service"). Ten voters were not sent their absentee ballots from the county in time to return them to be counted by the election deadline. (*See* Bailey Aff., Doc. 413 at 110-11; Broderick Aff., *id.* at 112-115.) Fourteen voters reported that they returned their absentee ballots by the deadline, but the Secretary of State's website indicates the ballot was not counted. A handful of voters received incomplete absentee ballots. (*See* Laurand Aff., Doc. 413 at 138-40.)

72 Defendants attempt to explain away these encounters by the voters by offering speculation that the better explanation is that there were "instances of user error or potentially poor viewing angles or long fingernails causing inadvertent touches to register with the machine." (State Defs.' Resp. at 34) (citing Ledford Dep. at 103-104)(testifying that she did not have any idea why the machine was incorrectly marking the voter's selection without being there, she did not know whether the voter touched something, if he had a big finger, or if he had something on him that touched the screen) (citing Doran Dep. at 79-80)(testifying that she is aware of a single issue with an older woman during early voting who used her fingertips or fingernails to make selections that were not registering on the machine). The Court acknowledges that there were undoubtedly some instances of poll worker and voter error. However, the Court finds that Defendants did not offer much – only bare assertions and the testimony noted here – to refute Plaintiffs' evidence of the experience of these voters at the polls.

73 This evidence contradicts the State Defendants' characterization that "[a]lmost none of these individuals raised these alleged issues with election officials." (State Defs.' Resp. at 31.)

74 The Court notes that in connection with the Coalition Plaintiffs' 2018 Motion for Preliminary Injunction similar evidence was presented for other couples living in the same address.

75 The Curling Plaintiffs' remedy would require Defendants to supply a minimum of one ballot marking device (BMD) per polling location for assistive voting by paper ballot that meets HAVA/ADA requirements that is voter verifiable. The Coalition Plaintiffs' remedy would allow the State to use its DREs for remaining elections for this purpose.

76 Under the Curling Plaintiffs' remedy, the Court could require the State to provide each county with precinct ballot scanners as provided under O.C.G.A. § 21-2-300, enacted April 2, 2019, mandating that "[t]he state shall furnish a uniform system of electronic ballot markers and ballot scanners for use in each county as soon as possible," if existing inventory of AccuVote OS scanners is insufficient for use in the remaining 2019 elections. The Coalition Plaintiffs' request would allow the counties to use their existing AccuVote OS scanners and leave it to the counties to determine whether to tabulate at the precinct or a central/county election office.

77 The Court notes that the State Defendants representations about the scope of the costs are overstated as they do not appear to account for the many municipalities that already use hand-marked paper ballots (i.e. 70 out of the 99 scheduled for Fall 2019) that are either scanned or hand counted.

78 The State Defendants indicate in the response brief that "[t]he entire budget for the Elections Division of the Secretary of State's Office is $6,118,907 for Fiscal Year 2020 in both state and federal funds, and the majority of those funds cover expenses like personnel or other items that could not be adjusted to hastily implement a new voting system." (Resp. at 60.) The Court notes that no testimony was offered by anyone from the Secretary of State's Office, via affidavit or at the hearing, as to the State's elections budget for this fiscal year. And, they further assert that requiring the State to purchase new voting equipment to be used only for the November 5, 2019 elections would likely necessitate the calling of a Special Session by the Governor to seek appropriation of additional state taxpayer dollars and that given the implementation timeline for the November 5, 2019 elections, there would not be sufficient time to purchase the equipment using bond funds, which are being used to purchase the new voting system contemplated by H.B. 316. These arguments ignore that Plaintiffs' relief does not require the purchase of equipment different from the equipment provided for in the State's chosen election system – optical paper precinct ballot scanners and ballot boxes, though it would require purchase of privacy booths (or dividers).

79 The State Defendants assert that the "Curling Plaintiffs propose scrapping the entirety of Georgia's current election system (including optical scanners), which would require the procurement of: (1) new ballot-building software and equipment, (2) at least one BMD for every precinct, (3) at least one optical scanner and secure storage box for every precinct, and (4) paper ballots" and that "Coalition Plaintiffs propose scrapping part of the existing system, which would still require procurement of: (1) new optical scanners for every precinct, (2) at least one BMD or DRE for every precinct, and (3) paper ballots." (*Id.* at 56.) The State claims that the "fiscal cost" of this relief is "staggering" (*Id.* at 56.) Again, these arguments fail to address the reality that the Curling Plaintiffs' proposed remedy (and to some extent the Coalition's remedy) would require the State to use the very same equipment it is purchasing under its contract

with Dominion – BMDs that print paper ballots and paper ballot scanners – and therefore would not require the purchase of additional equipment or the expenditure of additional funds beyond those approved in the original bond.

80 The State Defendants also presented testimony from Gwinnett County's Elections Division Director about the feasibility of a switch to paper ballots for the November 2019 elections. However, Gwinnett County is not conducting any county elections and has not contracted with any municipalities with scheduled elections in November. Consequently, were this Court to grant Plaintiffs' requested relief for the 2019 elections, there would be no impact on the current operations of the Gwinnett County Elections Division. Therefore, while Ms. Ledford has extensive experience with conducting elections in Gwinnett County, the Court finds her testimony to have limited relevance for this purpose.

81 Mr. Bridges considered two cost scenarios, one where the Court grants the Coalition Plaintiffs' remedy which permits the use of existing DRES for disabled voters under HAVA, and the other where the Court grants the Curling Plaintiffs' request that BMDs be purchased for this purpose. (Tr. Vol.2, Doc. 571 at 270) ("If we're looking at like -- for example, if we went with the BMD-type system, it is about $900,000. Or if we were looking at, you know, acquiring current technology equipment, we are probably looking at half-a-million-dollar expenditures, neither of which I have the money for.") However, he acknowledged that the State is responsible for purchasing the BMDs under its new system. (*Id.* at 261.)

82 Mr. Bridges used a price of $5,000 per scanner for his estimate based on a study by the Brennan Center for Justice regarding the cost of new scanning machines. (Tr. Vol.2, Doc. 571 at 261-62; Bridges Decl. at 6.)

83 This testimony differs from the Declaration of Joseph Blake Evans, the Elections Chief of the Fulton Co. Department of Registration and Elections who stated that the budget for the September 2019 elections is $696,932. (Decl. of Joseph Blake Evans, Doc. 473-1 ¶ 12.)

84 Poll workers are however familiar with handling provisional paper ballots (*Id.* at 229.)

85 This estimate was based on using one scanner per precinct. (*Id.* at 335.)

86 The Coalition Plaintiffs also presented Declarations from Aretha Hill and Marion Warren, the Election Superintendent and Registrar/Absentee Ballot Clerk for the City of Sparta respectively that: (1) they have concerns about the security and reliability of the current electronic voting system and DRE machines, and (2) the City of Sparta is ready and capable of conducing paper ballot elections in 2019 with their existing equipment or by hand count. (Decl. of Aretha Hill, Doc. 507, Ex. C; Decl. Marion Warren, Doc. 507, Ex. D.)

87 Finley was also appointed as the California Secretary of State's representative on the Standards Board of the Federal Election Assistance Committee, charged with developing standards applied for certification at the federal level of all voting systems. (*Id.* at 34.)

88 Not all counties in California used DREs as a voting method.

89 According to Mr. Finley the state needs one BMD device at each precinct conducting elections to comply with HAVA. This would be feasible because the state is already planning to have multiple BMDs at the precincts in counties in the pilot program. (*Id.* at 51-52.)

90 McReynolds administered elections in Denver, Colorado for over thirteen years and was the Director of Elections for seven years. (July 25, 2019 Tr., Doc. 570 at 117-18.) McReynolds is currently the Director of the National Vote at Home Institute. (*Id.*)

91 Cuyahoga County is one of the nation's most populous electoral jurisdictions – approximately the 11th largest – with more registered voters than some State's entire voting population. The County conducts elections for 59 entities (such as school boards and library taxing districts) in addition to holding major Federal, State, and local contests. (Decl. of Cadice Hoke ¶ 18, Doc. 413, Ex. E.)

92 Professor Hoke holds a J.D. from Yale Law School and a Master's Degree of Science in Information Security Policy and Management from Carnegie Mellon University. (*Id.* ¶ 6.) Hoke has testified before the elections oversight committee of the U.S. House of Representatives on the importance of conducting independent post-election audits and advised federal government officials at the Pentagon, the Executive Office of the President, DHS and the Election Assistance Commission on election security vulnerabilities, including that the U.S. election administrative system be designated as part of critical infrastructure. (*Id.* ¶¶ 14-15.) According to her CV, she was a Law Professor at Cleveland State from 1994-2017 and now works in private practice as a consultant on "Operational Security and Cyber Risk Assessments." (*Id.*)

93 In *Bonner v. City of Prichard*, 661 F.2d 1206, 1209 (11th Cir. 1981) (en banc), the Eleventh Circuit adopted as binding precedent all of the decisions of the former Fifth Circuit rendered prior to the close of business on September 30, 1981.

94 *See also* discussion in *Curling* of *Stewart* and *Wexler v. Anderson*, 452 F.3d 1226 (11th Cir. 2006) relative to the posture of the instant case. *Curling*, 334 F. Supp. 3d at 1325.

95 As discussed herein, this assumes the State's implementation of the BMD system goes off without a hitch. (The Court also notes that the question of "rollout without a hitch" means that the new system has been fully implemented in all counties, that the equipment actually functions in conformity with contractual requirements, and that elections staff are able to operate the system properly and conduct at least preliminary audits based on comparative reviews of the paper ballots and scanner tabulations.)

96 The Court is not suggesting that defense counsel made an intentional misrepresentation in this connection – but only that there appears to be schedule slippage in an already tight statewide rollout framework

97 According to the elections chart submitted by the State, Evans County has no scheduled elections and the four municipalities in Evans County conduct their own elections by lever or paper ballot.

98 The approximate overall populations of these counties are: Bacon (11,319), Bartow (105,054), Carroll (117,912), Catoosa (66,550), Charlton (12,715), Decatur (26,716), Evans (10,775), Lowndes (115,489), Paulding (159,445), and Treutlen (6,740).

99 *See also* discussion of testimony of Amber McReynolds, *supra*, regarding her concerns about the aggressive time frame for the state's rollout which she viewed as more condensed than in any other states that have launched statewide election system changes.

100 Counties or jurisdictions where one or more municipalities are already using hand-marked paper ballots or other jurisdictions that have had experience with hand-marked paper ballot voting in the past may provide the easiest viable candidates at this juncture.

101 This injunctive relief is consistent with the findings of the National Academies of Science Report detailing the various methods in which contamination of voter registration data and electronic pollbooks used in conjunction with voting systems disrupts elections and its recommendation that all jurisdictions using electronic pollbooks "should have backup plans in place to provide access to current voter registration lists in the event of any disruption." (NAS Report at 72.)

102 As discussed at length in this Order, the premier 2018 Report of the National Academies of Sciences, Engineering, and Medicine recommends the use of paper ballots based on its finding that "[c]omplicated and technology-dependent voting systems increase the risk of (and opportunity for) malicious manipulation." (NAS Report, Doc. 285-1 at 128.)

103 Quotation attributed to Yogi Berra.

End of Document

May 10, 2018

The Honorable Rolando Pablos
Secretary of State
1100 Congress
Capitol Bldg., Room 1E.8
Austin, Texas 78701

Keith Ingram, Director of Elections
Secretary of State, Elections Division
James E. Rudder Bldg.
1019 Brazos St.
Austin, Texas 78701

CC: The Honorable Bryan Hughes, Chair, Senate Select Committee on Election Security
The Honorable Jane Nelson, Chair, Senate Select Committee on Cybersecurity
The Honorable Giovanni Capriglione, Chair, House Select Committee on Cybersecurity

Re: Cybersecurity and Election Security Recommendations

Dear Secretary Pablos and Director Ingram,

As computer scientists and cybersecurity experts at some of Texas's most preeminent academic and research institutions, we write to outline reasonable, but critical, measures that Texas must undertake to make its elections more secure and reliable. An accurate, secure election system is -- and absolutely must be -- a nonpartisan goal. Nothing could be more critical to our American democracy, or to Texans' faith in the elections process. Below, we lay out four key priorities: (1) updated election security standards and accountability mechanisms, (2) auditable paper trails, (3) mandatory post-election audits, and (4) secure voter registration systems.

Two impending events make outspoken leadership from your office an urgent matter. First, Texas will very shortly receive approximately $23.3 million dollars in federal funding earmarked specifically for improving election security.[1] The money may be used to replace voting equipment with machines that provide a voter-verified paper record, implement a post-election audit system, upgrade election-related computer systems to address cyber vulnerabilities, facilitate cybersecurity training for election officials, or implement cybersecurity

[1] Financial Services And General Government Appropriations Bill, 2018, Omnibus Agreement Summary, *available at* https://www.appropriations.senate.gov/imo/media/doc/FY18-OMNI-FSGG-SUM.pdf; Brennan Center for Justice & Verified Voting, *Federal Funds for Election Security: Will They Cover the Costs of Voter Marked Paper Ballots?* (Mar. 2018), *available at* https://www.verifiedvoting.org/wp-content/uploads/2018/03/Federal_Funds_for_Election_Security.pdf.

best practices for election systems.[2] It is crucial that this funding be spent effectively and as part of a comprehensive plan for updating and securing Texas's election systems.

Second, under the Texas Cybersecurity Act, the Secretary of State's office must conduct a study of cyber attacks on election infrastructure by December 1, 2018.[3] We understand that Director Ingram is spearheading this process. The study must include an investigation of vulnerabilities and risks for a cyber attack against Texas's voting and voting registration systems, information on any attempted cyber attack on these systems, and "recommendations for protecting a county's voting system machines and list of registered voters from a cyber attack."[4] As cybersecurity experts and Texas voters, we feel a duty to ensure that your recommendations reflect the best research and analysis of existing technology and its vulnerabilities.

Election security represents a profound challenge to both our democracy and our national security -- one we are confident Texas can meet with its typical innovative spirit. Other states are addressing this challenge with creative policy solutions[5]--but Texas still has an opportunity to be a leader. We urge you to use the mandated report as an opportunity to recommend meaningful and technically-sound updates to our state's systems -- and, if necessary, use your statutory authority to issue updated voting systems standards. Below, we offer four specific policy recommendations that will improve the security, reliability, and transparency of Texas voting and voter registration systems. Some of these represent critical improvements that must be implemented with all due haste.

BACKGROUND

Texas's 254 counties employ an array of election systems, with voting methods ranging from hand-marked paper ballots to direct-recording electronic (DRE) voting machines. In the 2016 election, approximately 148 counties used some or all paperless DRE machines, which produce no auditable paper trail.[6] This includes Harris County, which has over 2.2 million registered voters and uses entirely paperless DRE machines for election day voting.

A number of the machines currently employed in Texas have known security vulnerabilities, exacerbated by lack of an auditable paper trail.[7] Our state's voting machine

---

[2] Staff of H. Comm. on Appropriations, 115th Cong., Joint Explanatory Statement on Financial Services and General Government Appropriations Act, 2018 (2018), http://docs.house.gov/billsthisweek/20180319/DIV%20E%20FSGG%20SOM%20FY18%20OMNI.OCR.pdf.

[3] Tex. Elec. Code § 276.011(a)(1).

[4] Tex. Elec. Code § 276.011(b)(1)-(3).

[5] Bennett Leckrone, *Ohio Senate OKs $115 million to help counties replace voting machines*, The Columbus Dispatch (April 12, 2018), *available at* http://www.dispatch.com/news/20180412/ohio-senate-oks-115-million-to-help-counties-replace-voting-machines; Press Release, "Department of State Tells Counties to Have New Voting Systems in Place by End of 2019" (April 12, 2018), Pennsylvania Department of State, *available at* http://www.media.pa.gov/Pages/State-Details.aspx?newsid=276.

[6] Verified Voting, *The Verifier - Polling Place Equipment - November 2016*, *available at* https://www.verifiedvoting.org/api?advanced&state_fips=48&equip_type=&make=&model=&year=2018&download=excel.

[7] *See, e.g.*, Adam Aviv *et al.*, *Security Evaluation of ES&S Voting Machines and Election Management System*, *available at* https://www.usenix.org/legacy/event/evt08/tech/full_papers/aviv/aviv.pdf (ES&S iVotronic interface);

security is further undermined by the age of the equipment in use today. Equipment in many Texas counties is over a decade old. For example, Bexar County's 2,842 DRE machines, which have no verifiable paper trail and serve over 1 million registered voters, were purchased in 2002.[8] We must assume that adversaries have had plenty of time to devise attacks on these machines, many of which are obsolete. In some cases, manufacturers no longer make replacement parts or provide security updates for critical components. Texas voter registration systems -- forty separate databases in total -- are particularly vulnerable as they are networked and largely unregulated at the state level.

It is no longer sufficient to rely on physical protection of our election infrastructure: secure elections require "defense in depth" to ensure that they can be robust in the face of misconfigurations, misunderstandings, and malice. Texans deserve modernized and cyber-secure voting systems. It is time to plan for the necessary expense of retiring Texas's outdated and insecure voting technology, and replacing it with equipment that better satisfies cybersecurity best practice standards. This will take forethought, and it will take legislative and executive action. The security concerns described below are very real, and it is important that Texas proceed to address them.

Although our current voting systems are aging and insecure, Texas must balance the need to act quickly with the need to ensure that new systems meet better standards than are currently in place. Our state leaders, including your office, must prioritize smart and forward-looking expenditures grounded in the best available research. Like any essential state function, there is a cost to securing Texas elections. But the cost is not insurmountable, and it is money very well spent. As an initial matter, the recently-allocated federal funding, if deployed effectively, can help with short-term planning and preparations between now and the November 2018 election.

RECOMMENDATIONS

Below, we lay out four specific policy recommendations that will improve the security, reliability, and transparency of Texas voting and voter registration systems. As a general matter, we see two overarching priorities: improving statewide standards to ensure election security going forward, and replacing Texas's aging, outdated, and vulnerable voting systems in conformance with these standards. ***The order of operations here matters***: there must be improved standards in place before new voting machines are purchased. The reason is simple: if we allocate money before standards are in place, counties and the state will invest significant resources on inadequately secure voting machines that will, for all practical purposes, be

---

Matt Blaze & Jake Braun, *DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure* (Sept. 2017), *available at* https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf (Premier AccuVote TSx, ES&S iVotronic interface); Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine* (2006), *available at* https://s3.amazonaws.com/citpsite/publications/ts06full.pdf.

[8] Jacquelyn Callanen, *How Bexar County elections officials protect Texans' votes*, Trib Talk, a publication of the Texas Tribune, (Oct. 24, 2016), *available at* https://www.tribtalk.org/2016/10/24/how-bexar-county-elections-officials-protect-texans-votes/.

grandfathered in under the current standards.[9] The problems identified above will be replicated for another decade -- or more. This reality deserves especial emphasis in light of Texas's imminent receipt of federal funding from March's omnibus federal spending bill.

These recommendations are based on our collective expertise, years of research, and best practices articulated by leading independent research organizations. Together, these recommendations describe a system of election administration that provides reasonable cybersecurity. We urge you to include these recommendations in your report to the Legislature on December 1, 2018, and to use your statutory authority to ensure that as many of these changes are in place as early as possible. We stand ready to lend our expertise to the drafting and implementation of updated standards.

1. **Your office, and the Legislature, should design and implement protective and proactive election cybersecurity standards and accountability mechanisms that ensure statewide compliance with best practices.**

Laws and regulations must be in place to ensure consistent cyber-hygiene throughout Texas's election system. This includes not just voting machines, but voter registration systems, electronic poll books, IT infrastructure, and any other system whose disruption could alter the vote, alter who is able to vote (e.g., by changing registration records), sow confusion on election day (e.g., by causing machines to crash), or otherwise undermine Texas's ability to hold fair and reliable elections. You need not start from scratch; independent research organizations have developed comprehensive best practices that need only be translated into regulatory language.[10] Many of these standards can and should be in place before the November 2018 election.

Two narrow but necessary improvements are worth mentioning here. First, the State of Texas does not currently require election officials to undergo cybersecurity training. Last year's Verizon's Data Breach Investigation Report (DBIR), which analyzed 1,935 actual security breaches reported by sixty-five partner organizations, noted that "1 in 14 users were tricked into following a link or opening an attachment—and a quarter of those went on to be duped more than once" and "80% of hacking-related breaches leveraged either stolen passwords and/or weak or guessable passwords."[11] Untrained or careless end-users are typically the greatest security vulnerability. Even otherwise tech-savvy users can be manipulated into compromising a network if they lack proper security awareness. Texas should require cybersecurity training for county and local election officials so that they aren't tricked into allowing bad actors into county and state systems.

---

[9] *See* Tex. Elec. Code §§ 122.001(a)(3), 122.031(a), 122.032(a); 1 Tex. Admin. Code §§ 81.60, 81.61.

[10] For example, see Verified Voting Foundation, Principles for New Voting Systems, *available at* https://www.verifiedvoting.org/voting-system-principles/ (listing ten key principles to which every voting system should conform); Center for Internet Security, A Handbook for Elections Infrastructure Security (Feb. 2018) at 36-66, *available at* https://www.cisecurity.org/elections-resources/ (detailing best practices to address risks to elections systems, categorized by priority (high to low), cost, and connectedness class (network connected, indirectly connected, or transmission)).

[11] 2017 Verizon Data Breach Investigations Report (10th Ed. 2017), *available at* http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

Second, Texan voters stationed or living overseas must not be allowed to return voted ballots electronically, as is currently allowed for overseas military voters in Bexar County. As Professor Dan Wallach testified on February 22, the Internet "makes it much easier for nation-state adversaries to attack our elections . . . . Safe internet voting is simply not feasible today. . . particularly in light of the threats these systems will face."[12] There is presently no way to economically and adequately secure votes submitted online--but there are other ways to ensure Texas military members are able to vote.

In addition to a legislative solution, your office can prescribe additional standards for voting systems beyond the basic requirements laid out in Texas Election Code § 122.001(a). The standards can apply to particular kinds of voting systems, particular elements comprising a voting system, or to voting systems generally.[13] At the earliest practicable time -- but no later than necessary to implement improvements in advance of the 2020 election -- we urge you to use this statutory authority to ensure that Texas voting systems meet the highest possible cybersecurity standards.

Additionally, the legislature should grant the Secretary of State sufficient authority to ensure that *all* Texas voters enjoy access to voting systems equipped with adequate safeguards. As Director Ingram repeatedly testified at the Senate Select Committee on Election Security's February 22, 2018 hearing,[14] the Texas Secretary of State lacks the authority to enforce substantive provisions of the Election Code. Although legislative solutions are necessary, updated election security requirements will be meaningless if there is no way to hold counties -- and vendors -- accountable for compliance. There must be a system in place to ensure that modernized, effective standards are uniformly followed. Therefore, we suggest your recommendations include a provision allowing the Secretary of State's office to enforce the standards issued by that office as well as those provisions of the Election Code governing election equipment, voter registration, and cybersecurity training. To this end, your office should also recommend a provision requiring that voting system manufacturers notify the Secretary of State of known security breaches and malfunctions, and provide a penalty for failing to do so.[15]

2. Texas should immediately adopt voting systems standards that require a paper record of every vote cast in every election in Texas, and replace paperless machines with machines that produce a voter-verified paper record.

---

[12] *Hearing Before the S. Select Comm. on Election Cyber Security*, 85th Interim Sess. (Tex. 2018) (statement of Dr. Dan Wallach, Professor of Computer Science, Rice University), *available at* https://www.cs.rice.edu/~dwallach/pub/texas-senate-feb2018.pdf.

[13] Tex. Elec. Code §§ 122.001(c), 122.032(b).

[14] Video Recording: Hearing Before the S. Select Comm. on Election Cyber Security, 85th Interim Sess., (Tex. 2018), *available at* http://tlcsenate.granicus.com/MediaPlayer.php?view_id=44&clip_id=13172.

[15] In early 2018, Washington State introduced legislation that would require manufacturers of voting system equipment to report certain security breaches on their equipment to the Secretary of State and State Attorney General. 2017 WA H.B. 2388. If a voting system manufacturer fails to meet this notice requirement, the Secretary of State must decertify that manufacturer's voting systems. The proposed law also gives the Secretary of State power to decertify a voting system and withdraw authority for its future use or sale in the state if, at any time after certification, the secretary of state determines that it fails legal requirements. *Id.* Colorado requires similar notice of malfunctions; failure to provide notice is grounds for decertification. 8 Colo. Code Regs. § 1505-1:11.

Every vote cast in Texas should produce a voter-verified paper audit trail ("VVPAT") that becomes the official record of the vote cast in the case of a recount or dispute. Paper records (collected in a secure, private way) are indispensable to a secure elections system. A much-touted defense against cyberattacks is the "air gap" around physical infrastructure that physically separates equipment from the Internet. Indeed, Texas should mandate that all infrastructure is truly air-gapped, and that no remote access software has been installed on machines or pollbooks. However, even those voting machines with a physical "air gap" are not impenetrable against unauthorized or malicious access. To the contrary, nation state adversaries have devised a number of workarounds, which have been used to, for example, damage nuclear centrifuges that use similar air gap defenses.[16] Election management software may be an especially viable attack vector.[17] The best mitigations we have for the systems Texas uses today are only possible where there is a paper voting record.

If voting machines in any of the 148 Texas counties that still either fully or partially rely on paperless DRE machines were attacked, it is very unlikely that they would show any evidence of it. By way of example, in the recent Dallas Democratic primary for District Attorney, if merely a handful of the county's 1,250 iVotronic DRE machines were compromised, the outcome (a 584 vote margin out of 112,701 cast[18]) could have been swung in either direction. While no such attacks in that race are suspected, in the event that allegations were made, the Dallas County Elections Department would have been unable to verify the outcome with meaningful certainty. Similarly, in a special election held recently in Pennsylvania's 18th Congressional District, the Republican candidate lost by 758 votes out of over 227,000 cast.[19] Had either side sought a recount, it would not have been possible to conduct a meaningful one due to the lack of any paper trail. Maintaining paper ballot records as a backup is key to election legitimacy: where machines or systems have been attacked, paper ballots provide a far more secure and easily audited record of the vote.[20]

VVPAT can take many forms: an old-fashioned paper ballot filled out by hand; paper ballot filled out by the voter and tabulated by an optical scanning machine; or a printed receipt of votes cast on a DRE machine that the voter uses to confirm that his or her vote was cast correctly. In whatever form, VVPATs safeguard against cyberattacks by providing a non-digital

---

[16] *See, e.g.*, Ralph Langner, To Kill A Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve (Nov. 2013), *available at* https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.
[17] Eric Chabrow, *Intelligence Panel Learns How to Hack Air-Gapped Voting Systems*, Bank Info Security (June 21, 2017), *available at* http://www.bankinfosecurity.com/intelligence-panel-learns-how-to-hack-air-gapped-voting-systems-a-10030.
[18] Tasha Tsiaperes, *There Will Be No Recournt in the Dallas DA Democratic Primary*, Dallas Morning News (March 20, 2018), *available at* https://www.dallasnews.com/news/2018-elections/2018/03/19/will-no-recount-dallas-da-democratic-primary.
[19] Wes Venteicher, *Conor Lamb's lead grows as special election review continues*, Trib Live (March 20, 2018, 4:15 PM), *available at* http://triblive.com/local/regional/13443796-74/conor-lambs-lead-grows-as-special-election-review-continues
[20] Michael Miller, *How the U.S. can prepare for a major election hack*, The Washington Post (March 15, 2018), *available at* https://www.washingtonpost.com/news/monkey-cage/wp/2018/03/15/how-the-u-s-can-prepare-for-a-major-election-hack/?utm_term=.5e3de8bd1f13&wpisrc=nl_politics&wpmm=1.

artifact reflecting the voter's intent that can be subject to audits and recounts as needed to ensure that election results are accurate. However, importantly, paper ballot and optical scanner-based systems are considerably less expensive than DRE-based systems: last year Cameron County replaced its aging equipment with paper ballots and optical scanners for about $12 per registered voter.[21] Based on our examination of recent purchases in eight Texas counties, the total cost of new DRE voting machines averaged $16.42 per registered voter. Operating costs for optical scan machines are also typically lower.[22]

There are two realistic, more secure voting machine options available today. First, *next-generation optical scan systems*, specifically precinct-based optical scan systems. These systems involve hand-marked ballots that are scanned at the ballot box. Although optical scan systems face cyber threats, paper ballots enable robust paper audit procedures. Some Texas counties, Denton County included,[23] already use this technology.

Second, *next-generation hybrid voting systems*, such as Los Angeles County's Voting Systems Assessment Project and Travis County's STAR-Vote,[24] generate printed paper ballots which can be tallied electronically or by hand. These systems use sophisticated cryptographic security techniques[25] and allow for risk-limiting audits,[26] described in more detail below. A key benefit of bespoke systems like these is that the hardware (the physical machine, including screen and printer) and voting software are unbundled; software can be updated without purchasing new equipment (and vice versa), and off-the-shelf hardware can be repaired with commercially-available products. Texas is a great engine for innovation in many fields, and the field of voting technology need be no different.

---

[21] The total cost of the new machines was $2.5 million in Fall 2017, and Cameron County had 201,020 registered voters as of March 2018. *See* Frank Garza, *New Voting Machines to be More Efficient, Secure*, The Brownsville Herald (Oct. 7, 2017), *available at* http://www.brownsvilleherald.com/premium/article_ebdc8660-abcf-11e7-9900-6f329a8b88e1.html; Texas Secretary of State, *March 2018 Voter Registration Figures*, *available at* https://www.sos.state.tx.us/elections/historical/mar2018.shtml.

[22] Verified Voting, "Are verified paper ballots cost effective?", *available at* https://www.verifiedvoting.org/downloads/Newvvpbcosts.pdf.

[23] Emma Plattoff, *Denton County going to all-paper ballots for November*, Star-Telegram (July 4, 2017, 2:14 PM), *available at* http://www.star-telegram.com/news/politics-government/election/article159587389.html.

[24] *See* Voting Systems Assessment Project: Phase III: System Design and Engineering (2017), *available at* http://vsap.lavote.net/wp-content/uploads/2017/08/VSAP-Phase-III-Report.pdf; Susan Bell *et al.*, STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System (2013), *available at* http://traviscountyclerk.org/eclerk/content/images/presentations_articles/cuc_presentation/pdf_tc_elections_8_dans_star2013_presentation_paper.pdf. For more details on how STAR-Vote works, see a video and technical paper at https://www.usenix.org/conference/evtwote13/workshop-program/presentation/bell.

[25] What can sophisticated cryptography do? Cryptography, used properly, provides mathematical transformations of ballots that can protect the privacy of votes while simultaneously allowing any election observer to verify that votes were "counted as cast" (i.e., that the individual votes, posted in public, add up to the correct totals) and that the votes were "cast as intended" (i.e., that potentially malicious voting machines would be caught if they tried to substitute votes for other candidates than the voters intended).

[26] *See, e.g.*, Mark Linderman & Philip B. Stark, *A Gentle Introduction to Risk-limiting Audits*, IEEE Security And Privacy, Special Issue On Electronic Voting (Mar. 2012), *available at* https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

One option your office could consider recommending is centralizing the creation and management of innovative and cost-effective voting systems in the vein of STAR-Vote. While there are some benefits to a decentralized system where each county independently purchases and manages its voting systems, centralization would enable significant cost savings, facilitate maintenance and customization, make replacing failed or obsolete equipment much easier, improve security and reliability, and allow for quick and affordable adoption of technological improvements. Moreover, if the design, data formats, and programming interfaces are sufficiently open, there can be a competitive market for support services, including configuration, maintenance, integration, and customization.

Both optical scan and hybrid systems conform with independently-developed best practices for modern voting systems.[27] ***Most importantly, whatever machines Texas adopts must provide voters with the means and opportunity to verify human-readable marks on paper that correctly represent their intended selections, before casting their ballot, and preserve vote anonymity.*** Ideally, Texas voting systems should be such that county elections officials should be able to configure, operate, and maintain the system, create ballots, tabulate votes, and audit the accuracy of the results without relying on external expertise or labor, even in small counties with limited staff.

3. Texas should require post-election audits for all elections in all jurisdictions and, in particular, implement the best practice of risk-limiting audits.

Texas should require mandatory post-election audits,[28] with clear rules for the methodology and size of the audits, and the point at which audit results trigger a larger audit or full-scale recount. Currently, Texas law only requires post-election audits in jurisdictions using paper ballots.[29] The law also provides the Secretary of State with discretion to audit in jurisdictions using electronic voting systems.[30] This is manifestly insufficient in today's cyberthreat environment. Like VVPATs, clear and rigorous audit procedures safeguard against hacks by creating a statistically-sound method for detecting anomalies and a policy for overriding electronic tabulations if they become unreliable. It bears emphasis that ensuring appropriate audit practices means also ensuring that all jurisdictions use VVPATs. Without a paper record, meaningful audits are impossible.

---

[27] *See, e.g.*, Verified Voting Foundation, Principles for New Voting Systems, *available at* https://www.verifiedvoting.org/voting-system-principles/.

[28] In 2017, Colorado became the first state to implement mandatory risk-limiting audits. *See* C.R.S.A. § 1-7-515 (2)(a). Rhode Island subsequently passed a bill mandating risk-limiting audits beginning in 2020. 17 R.I. Gen. Laws § 17-19-37.4. Other states, including California, Oregon, and Utah, require mandatory post-election audits. *See, e.g.*, Cal. Elec. Code § 15560; O.R.S. § 254.529; Office of the Lieutenant Governor, "Election Policy," § 6.2 (Oct.17, 200), *available at* https://www.verifiedvoting.org/wp-content/uploads/2017/03/ElectionXPolicy.pdf.

[29] Texas law requires that the audit is done by a "manual count." Tex. Elec.Code § 127.201(a). However, many Texas precincts use direct-recording electronic machines (DREs) without a voter-verified paper audit trail (VVPAT), meaning that no hand count of ballots or VVPATs can be conducted in those precincts. And indeed, the audit statute explicitly provides that the hand count requirement does not apply where DREs are used. *See* Tex. Elec. Code §127.201(g).

[30] Tex. Elec. Code § 43.007(c).

In particular, the clear best practice is to require risk-limiting audits of the sort now required in Colorado.[31] This procedure increase voter confidence that election outcomes are correct and can help counties discover and correct procedural mistakes. A risk-limiting audit is an "audit protocol that makes use of statistical methods and is designed to limit to acceptable levels the risk of certifying a preliminary election outcome that constitutes an incorrect outcome."[32] The number of ballots included in an audit should be a statistically significant number tied to the margin of victory, not a fixed number as currently called for under Texas law. [33] To be at all meaningful, audits should be binding on the outcome of elections, and the discovery of an error should have an impact.

4. Voter registration systems, a weak link in Texas's election security, should be certified as secure, redundant, and accurate.

There are numerous threats to Texas's hybrid voter registration system, which aggregates thirty-nine locally-managed county databases with additional data from the 215 counties that are centrally managed. This hybrid system stores the records of over fifteen million voters. In many ways, this system represents the most critical and scalable target of our election infrastructure, because it includes 100% of the potential votes in any Texas election. As Senator Marco Rubio recently highlighted in a U.S. Senate Select Committee on Intelligence hearing, a foreign power could "penetrate the voter database of local election officials and strategically located counties or states, and . . . go into the database and they change the addresses of individuals, thereby their precincts move around, maybe they even delete some people from the rolls."[34]

Even a redesigned voter registration system would still, by necessity, require Internet connection so voters can verify their correct polling places, see sample ballots, and so forth. Most notably, during Texas's early voting period, we need an online database to track which voters have cast ballots. The mere fact that voter registration databases are network-connected (that is, online) results in a significant increase in vulnerability and risk. There are well known best practices to mitigate these risks, but "the ability to attack and manipulate voter registration systems by remote means makes them a priority for strengthening of the security resilience of these components."[35] These most vulnerable links in Texas's election security chain must be strengthened as soon as is practicable.

---

[31] Colorado Secretary of State, Understanding Risk Limiting Audits, *available at* https://www.sos.state.co.us/pubs/elections/VotingSystems/riskAuditFiles/UnderstandingRiskLimitingAudits.pdf. *See also* Center for Internet Security, A Handbook for Elections Infrastructure Security (Feb. 2018) at 28-29, *available at* https://www.cisecurity.org/elections-resources/.

[32] Colo. Rev. Stat. § 1-7-515. *See also* 8 Colo. Code Regs. § 1505-1:25 (detailing risk-limiting audit procedures).

[33] *See* Tex. Elec. Code § 127.201(a) ("To ensure the accuracy of the tabulation of electronic voting system results, the general custodian of election records shall conduct a manual count of all the races in at least one percent of the election precincts or in three precincts, whichever is greater, in which the electronic voting system was used").

[34] *Hearing on Election Intelligence Before the S. Select Comm. on Intelligence,* 115 Cong. (2018) (statement of Sen. Marco Rubio), *statements also available at* https://www.rubio.senate.gov/public/index.cfm/press-releases?id=0E99BF69-9CF4-460B-B911-046E7384665F.

[35] Center for Internet Security, A Handbook for Elections Infrastructure Security (Feb. 2018), *available at* https://www.cisecurity.org/elections-resources/.

Certification of Voter Registration and Management Systems

The Legislature must expand the responsibilities of the Texas Secretary of State's role in certifying voting systems to include the certification of voter registration and management systems. Counties that determine that subsequent, necessary security upgrades and practices are too costly could migrate to the statewide system. Specific requirements for such certification might include those listed in the National Research Council's "Improving State Voter Registration Databases,"[36] or the more recent recommendations issued by the U.S. Computer Emergency Readiness Team in their memo "Securing Voter Registration Data" memorandum.[37] The requirements will need to evolve regularly to keep pace with the threat landscape, so a flexible administrative framework that can be regularly updated is preferable to static set of rules/technical specifications.

As initial steps, Texas must establish baseline computer security standards for network firewalls, intrusion detection systems, and other "good hygiene" practices. The state should also consider centralizing the creation and management of voter registration tools, which would allow for more intensive and comprehensive cybersecurity reviews, and might aid in detecting anomalous changes to voter information. And, Texas should consider engaging independent third party vendors to provide ongoing services such as security assessments, vulnerability scanning and patching, penetration testing, and infrastructure monitoring and management.

Disaster Recovery/Continuity Planning

Something as massive as a hurricane or minor as a burst pipe above a server room could derail the administration of an election. Cyber attacks are also a form of disaster, and can have equally catastrophic effects. For example, Atlanta's city services were recently hobbled for a week over a ransomware attack aimed at simply extorting $51,000 in Bitcoins.[38] In the same week, Baltimore's 911 and 311 services were partially disabled by a separate attack.[39]

To mitigate risk from any of these potential events, the state should mandate that all critical server infrastructure related to voter databases (and, indeed, all election-related servers) should be capable of both local and offsite failover (the ability to switch to a redundant system during a failure) and snapshotting (the ability to revert to a previous instance of a system), which should be tested on a regular schedule through mandated drills to ensure counties can rapidly recover from corrupted or offline systems. Offsite encrypted backups of voter registration data should be required weekly. In the case of a ransomware attack, these measures would allow a jurisdiction to restore their affected systems with minimal data loss or services impact. To a

---

[36]National Research Council: Improving State Voter Registration Databases: Final Report (2010), *available at* https://doi.org/10.17226/12788.

[37] United States Computer Emergency Readiness Team, *Security Tip (ST16-001): Securing Voter Registration Data* (Sept. 30, 2016), *available at* https://www.us-cert.gov/ncas/tips/ST16-001.

[38] Leada Gore, *Atlanta Computers Still Down 6 Days After Cyber Attack; Will City Pay Ransom?*, AL.com (Mar. 28, 2018), *available at* http://www.al.com/news/index.ssf/2018/03/atlanta_computers_still_down_6.html.

[39] Kevin Rector, *Baltimore 911 Dispatch System Hacked, Investigation Underway, Officials Confirm*, Baltimore Sun (Mar. 27, 2018), *available at* http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-911-hacked-20180327-story.html.

similar end, jurisdictions that use electronic poll books should also be required to have paper backups at each poll site on election day; this practice is currently voluntary.

CONCLUSION

Our voter registration, vote casting, and vote tabulation systems are not ready to rebuff attacks from nation-state adversaries or others determined to attack the accuracy of Texas elections. Concrete steps must be taken to shore up Texas's elections systems as soon as possible, and certainly before the 2020 election. Under the Texas Cybersecurity Act, your office has a key role to play: your recommendations, due on December 1, and your advocacy in support of meaningful action in the 2019 legislative session, can be instrumental in turning Texas into a model for secure, accurate, and fair elections.

We urge to ensure that any federal funding Texas receives is spent wisely and in accordance with the principles outlined above. We also urge you to include the above recommendations in your December report. Of course, each one of these recommendations could be the subject of a lengthy and technical memorandum explaining best available practices. Texas has a wealth of expert resources, including the undersigned, and we urge you take advantage of this fact by engaging with computer security, cybersecurity, and election infrastructure experts to hone the specific language of your recommendations over the course of the next seven months.

Texans deserve an election system they can trust. The federal Constitution gives states authority over the conduct of elections, and few of our state's responsibilities go more directly to the heart of our democracy. As Texans and computer scientists, we stand ready to assist in designing and implementing reasonable changes that will make a significant and lasting difference -- and make Texas a leading example of reliable, accurate, and secure elections practices.

For inquiries regarding this letter, please contact Dan Wallach <dwallach@rice.edu>, 713-348-6155.

Sincerely,

Scott Aaronson, Professor, University of Texas at Austin

Chris Bronk, Assistant Professor, University of Houston

Alvaro Cardenas, Assistant Professor, University of Texas at Dallas

Guofei Gu, Associate Professor, Texas A&M

Murat Kantarcioglu, Professor, University of Texas at Dallas

Jiang Ming, Assistant Professor, University of Texas at Arlington

Dan S. Wallach, Professor, Rice University

Brent Waters, Associate Professor, University of Texas at Austin

Greg White, Professor, University of Texas at San Antonio

*****_In alphabetical order; affiliation given for identification purposes only._