See page 34

493 F.Supp.3d 1264 (2020)

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

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

United States District Court, N.D. Georgia, Atlanta Division.

Signed October 11, 2020.

1267*1267 David D. Cross, Eileen M. Brogan, Pro Hac Vice, John P. Carlin, Lyle F. Hedgecock, Pro Hac Vice, Mary G. Kaiser, Robert W. Manoso, Veronica Ascarrunz, Catherine L. Chapple, Jane P. Bentrott, Marcie Brimer, Pro Hac Vice, Morrison & Foerster, LLP, Washington, DC, Robert Alexander McGuire, III, Pro Hac Vice, 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 Donna Curling, Donna Price, Jeffrey Schoenberg.

David R. Brody, Pro Hac Vice, Ezra David Rosenberg, Pro Hac Vice, Jacob Paul Conarck, John Michael Powers, Lawyers' Committee for Civil Rights Under Law, Washington, DC, Robert Alexander McGuire, III, Pro Hac Vice, Robert McGuire Law Firm, Seattle, WA, 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 Plaintiff Coalition for Good Governance.

Robert Alexander McGuire, III, Pro Hac Vice, Robert McGuire Law Firm, Seattle, WA, Bruce P. Brown, Bruce P. Brown Law, Cary Ichter, Ichter Davis, LLC, Atlanta, GA, John Michael Powers, Lawyers' Committee for Civil Rights Under Law, Washington, DC, William Brent Ney, Ney Hoffecker Peacock & Hayle, LLC, Lawrenceville, GA, for Plaintiffs Laura Digges, William Digges, III, Ricardo Davis, Megan Missett.

Alexander Fraser Denton, Joshua Barrett Belinfante, Kimberly K. Anderson, Brian Edward Lake, Carey Allen Miller, Vincent Robert Russo, Jr., Robbins Ross Alloy Belinfante Littlefield, LLC, Bryan Francis Jacoutot, Bryan P. Tyson, Diane Festin LaRoss, James A. Balli, Jonathan Dean Crumly, Sr., Loree Anne Paradise, Robert Dalrymple Burton, Taylor English Duma LLP, Atlanta, GA, for Defendants David J. Worley, Rebecca N. Sullivan, Seth Harp, Brad Raffensperger.

Bryan P. Tyson, Diane Festin LaRoss, James A. Balli, Jonathan Dean Crumly, Sr., Loree Anne Paradise, Robert Dalrymple Burton, Taylor English Duma LLP, Vincent Robert Russo, Jr., Robbins Ross Alloy Belinfante Littlefield, LLC, Atlanta, GA, for Defendant Ralph F. (Rusty) Simpson.

Alexander Fraser Denton, Joshua Barrett Belinfante, Kimberly K. Anderson, Brian Edward Lake, Carey Allen Miller, Vincent Robert Russo, Jr., Robbins Ross Alloy Belinfante Littlefield, LLC, Bryan P. Tyson, Diane Festin LaRoss, James A. Balli, Jonathan Dean Crumly, Sr., Loree Anne Paradise, Robert Dalrymple Burton, Taylor English Duma LLP, Atlanta, GA, for Defendant The State Election Board.

Cheryl Ringer, David R. Lowman, Kaye Woodard Burwell, Office of the Fulton County Attorney, Atlanta, GA, for Defendants Richard Barron, Mary Carole Cooney, Vernetta Nuriddin, David J. Burge, Aaron Johnson, The Fulton County Board of Registration and Elections.

Cheryl Ringer, Office of Fulton County Attorney, Atlanta, GA, for Defendants Mark Wingate, Kathleen D. Ruth.

OPINION AND ORDER

AMY TOTENBERG, United States District Judge.

I. Introduction and Overview

In the 1983 film Groundhog Day, weather man Phil Connors is doomed to repeat the same day over and over again: "I wake 1268*1268 up every day, right here, right in Punxsutawney, and it's always February 2nd, and there's nothing I can do about it." The Court can relate; it feels like it's February 2nd in Punxsutawney. But quite likely, the Court is not alone in this sentiment in many respects. Amidst the many other serious concerns facing the public in this challenging era, issues surrounding election system security, reliability, fairness, and the correct counting of votes continue on the forefront of citizen concerns. And so too, in turn, does voting litigation perforce continue.

Now in Act 4, this voting case raising fundamental First Amendment and Fourteenth Amendment constitutional claims is before the Court on Plaintiffs'[1] current Motions for Preliminary Injunction seeking relief before the November 3, 2020 general election. The Court held three days of hearings on Plaintiffs' motions and has reviewed the parties' extensive briefs and evidentiary submissions. The Plaintiffs' motions are identified and described below.

(a) The Curling Plaintiffs' August 19, 2020 Motion for Preliminary Injunction [Doc. 785] seeks to require Defendants "to conduct in-person voting in elections by a hand-marked paper ballot system" in combination with "provisions for pre-certification, post-election, manual tabulation audits of paper ballots and to independently check the accuracy of equipment and procedures used to tabulate votes ... based on well-accepted audit principles that assure a high probability that incorrect out-comes will be detected and remedied"; and

(b) The Coalition Plaintiffs' August 24, 2020 Motion for Preliminary Injunction on BMDs, Scanning and Tabulating, and Auditing [Doc. 809] seeks to require the State Defendants to: (i) refrain from forcing in-person voters to use ballot marking devices ("BMDs") and instead cause voters to use hand-marked paper ballots as the standard method for in-person voting; (ii) adopt scanning threshold settings for the Dominion optical scanners and vote review procedures that

will ensure all voter marks on mailed and hand-marked paper ballots are counted; and (iii) require election superintendents to conduct meaningful, effective pre-certification audits of scanned hand-marked paper ballots to ensure the correctness of election outcomes.

The Coalition Plaintiffs' Motion for Preliminary Injunction on Paper Pollbook Backups also sought related relief requiring the Secretary of State to direct county election superintendents to use paper backups of the electronic pollbook at each precinct polling location to facilitate issuance of regular or emergency ballots on election day in the event of voting machine breakdowns and mishaps, power outages, and associated long voter lines. (Doc. 800.) This Court's Order of September 28, 2020 (Doc. 918) addressed these issues at length and granted that separate motion.

Plaintiffs' motions challenge the State Defendants' mode of implementation of a new voting system enacted by the Georgia Legislature on April 2, 2019[2] and their ongoing use of software, data systems, policies and practices that allegedly burden and impede Plaintiffs' exercise of 1269*1269 their First and Fourteenth Amendment rights to cast ballot votes that will be reliably counted. The Plaintiffs allege that Defendants have failed to implement a constitutionally acceptable election system by requiring all in-person voters to use a BMD system that, as a whole, in its design and operation, is not voter-verifiable, secure, or reliable. They contend this system suffers from some of the same major cybersecurity vulnerabilities posed by Defendants' deeply flawed, out-dated Direct Recording Electronic ("DRE") Voting System addressed by the Court's lengthy Order of August 15, 2019 that granted injunctive relief.[3] (Doc. 579.) Plaintiffs' challenge embraces an array of associated issues involving the electronic voting process that impact if an individual's vote (whether recorded from a scanned BMD-generated barcode or a hand-marked paper ballot) will be correctly captured, scanned, and accurately counted.[4] Their claims thus also raise significant issues regarding the auditing of the election system's voting results and ballot processing.

First and foremost, Plaintiffs' challenge focuses on the Defendants' implementation of the new statewide BMD system, pursuant to the terms of the State's 2019 contract with Dominion Voting Systems.[5] The software and hardware system purchased provides for each citizen's BMD ballot vote selections to be printed on a paper ballot generated by a printer connected to the BMD. But the tabulation of the vote is actually based on the ballot's non-encrypted QR barcode on the ballot — designed to summarize the voter's ballot selections in code — that by itself is not voter reviewable or verifiable. Thus, Plaintiffs contend that the system precludes direct voter verification of the QR barcode of votes cast on the ballot. The printed ballot is fed into an ImageCast optical scanner that tabulates the ballot votes solely based on the QR code — and not based on the human readable text on the printed ballot. Plaintiffs challenge the constitutionality of the State Defendants' implementation of a barcode-based system for all in-person voting, based on (1) this alleged fundamental vote verification defect; (2) the system's purported known and demonstrated risk vulnerabilities to access and manipulation identified by national cybersecurity experts; and (3) the inherent problems posed in properly auditing votes tallied based on QR barcodes that cannot be verified by voters.[6]

1270*1270 Additionally, the Coalition Plaintiffs press their separate but related claim for relief based on the alleged intrusion on voters' free exercise of their right to cast a secret ballot at the

polls. The nature of this claim is two-fold. First, the Coalition Plaintiffs assert that in-person voters are required to make their ballot selections on oversized voting touchscreens that are not shielded and that expose the voter's ballot choices to easy viewing by other people in the precinct voting location. Second, they assert that a timestamping feature on the precinct scanner could be used to identify voters to reveal their vote choices.

As a whole, the State Defendants have steadfastly denied the factual and legal merits of Plaintiffs' constitutional claims. They argue that Plaintiffs have not carried their high burden of proof to show they are substantially like to prevail on their claims or their entitlement to relief under the rigorous legal standards for grant of a preliminary injunction.[7] Defendants have also urged the Court to per se deny all relief on the grounds that it would interfere with the State Defendants' authority and responsibility for oversight of election process and procedures, unfettered by burdens and confusion that can be caused by Court ordered changes to state election procedures or requirements on the eve of an election under *Republican Nat'l Comm. v Democratic Nat'l Com.*, ___ U.S. ___, 140 S. Ct. 1205, 1207, 206 L.Ed.2d 452 (2020) and *Purcell v. Gonzalez*, 549 U.S. 1, 4, 127 S.Ct. 5, 166 L.Ed.2d 1 (2006).

The General Election will be held on November 3, 2020. In-person early voting will proceed in select polling locations in every Georgia county from October 12, 2020 through October 30, 2020. While early voting in counties is done on BMD machines, the state still denominates these votes as "absentee" ballots. Under Georgia law, counties are authorized to begin sending out traditional paper absentee ballots this year on September 15, 2020 and to continue to do so thereafter in the weeks ahead prior to the election. The last date for submitting an application for an absentee mail paper ballot in Georgia is October 30, 2020. October 5, 2020 is the deadline for voter registration.[8]

Faced with this looming timeline, the Secretary of State just two weeks discovered a system-wide ballot display issue on the BMD touchscreen voting machines for the U.S. Senate special election with 20 candidates in the race. The Secretary of State designed the ballot using a two-column display to ensure that all 20 candidates appeared at the same time to voters on a single screen. Because BMDs primarily display candidates in a single column list, the two-column display is not a typical setup. Logic and Accuracy testing performed 1271*1271 on the BMDs by two counties in the last week of September revealed that the second column of candidates did not appear in some instances. Dominion engineered a software modification as a fix and within a few days the Secretary of State began distribution of the new software to counties for installation on all 30,000 plus BMDs before the start of early voting. Dominion submitted its application to the U.S. Election Assistance Commission ("EAC") for approval for the software engineering change on October 5, 2020 and secured the EAC's approval in a one sentence letter issued on October 9, 2020. EAC approval was secured after the modified software had been installed throughout the state.

Not surprisingly, the parties take wildly different positions on the magnitude of the problem and its impact on the general election. The State Defendants characterize this as a very minor issue and the fix as a de minimis change to the voting system software. Plaintiffs assert instead that the State is undertaking substantial changes to the election equipment two weeks before early voting begins without adequate testing that further jeopardizes the reliability and security of the

Dominion voting machines. These unforeseen circumstances, Plaintiffs insist, justify an emergency switch to hand-marked paper ballots.

Given the complex findings and analysis already covered by the Court's review of several lengthy preliminary injunction motions and issuance of related procedural orders over the last two years of intensive litigation, the Court refers the reader to its earlier orders for a further overview of the course of proceedings, relevant legal context, rulings, and factual findings. (*See, e.g.*, Doc. 309, September 17, 2018 Order (denying motion to dismiss and motion for preliminary injunction); Doc. 579, August 15, 2019 Order (granting in part preliminary injunction motions); Doc. 751, July 30, 2020 Order (granting in part and denying in part Defendants' most recent motion to dismiss including new BMD claims); Doc. 768, August 7, 2020 Order (denying without prejudice Plaintiffs' initial motions for preliminary injunction, Docs. 619 and 540, that facially challenged the BMD system and were filed in October, 2019, long prior to the 2020 election cycle, and summarizing case history).)

Finally, the Court notes that it has already addressed and rejected the State Defendants' renewed contention that several of Plaintiffs' requests for relief fall outside the bounds of the case as pled and presented to this Court. (*See, e.g.*, Order on Motion to Dismiss, Doc. 751 at 20-25; August 15, 2019 Order, Doc. 579 at 88-89.) Portions of the relief requested by Plaintiffs are clearly associated with their contentions regarding the Defendants' non-implementation of some of the relief granted in the Court's August 15, 2019 Order, as discussed in the Court's Opinion and Order issued on September 28, 2020. (Doc. 918.) Similarly, Plaintiffs have repeatedly advocated in their amended and supplemental complaints, motions, and briefs as well as at court hearings for the relief addressed in the current preliminary injunction motions before this Court.

II. Legal Standards

A. Preliminary Injunction Standard

A preliminary injunction is an "extraordinary remedy" designed to prevent irreparable harm to the parties during the pendency of a lawsuit before a final decision on the merits can be rendered. *See* *Winter v. Nat. Res. Def. Council*, 555 U.S. 7, 24, 129 S.Ct. 365, 172 L.Ed.2d 249 (2008). "A request for equitable relief invokes the district court's inherent equitable powers to order preliminary relief ... in order to assure the availability of permanent 1272*1272 relief." *Levi Strauss & Co. v. Sunrise Int'l Trading Inc.*, 51 F.3d 982, 987 (11th Cir. 1995); *Federal Trade Comm'n v. United States Oil and Gas Corp.*, 748 F.2d 1431, 1433-34 (11th Cir. 1984). To support a preliminary injunction, Plaintiffs must present evidence that clearly establishes: (1) a substantial likelihood of success on the merits on their claims; (2) a substantial threat of irreparable injury if the injunction were not granted; (3) that the threatened injury to the plaintiffs outweighs the harm an injunction may cause the defendants; and (4) that granting the injunction would not be adverse to the public interest. *McDonald's Corp. v. Robertson*, 147 F.3d 1301, 1306 (11th Cir. 1998). At the preliminary injunction stage, a district court "need not find that the evidence positively guarantees a final verdict in plaintiff's favor," and may rely on affidavits and hearsay materials which would not be admissible evidence for a permanent injunction, if the evidence is "appropriate given the character and objectives of the injunctive proceeding." *Levi Strauss & Co.*, 51 F.3d at 985 (quoting *Asseo v. Pan American*

Grain Co., 805 F.2d 23, 26 (1st Cir. 1986)); *McDonald's Corp.*, 147 F.3d at 1306 (11th Cir. 1998).

Federal courts "possess broad discretion to fashion an equitable remedy." *Black Warrior Riverkeeper, Inc. v. U.S. Army Corps of Engineers*, 781 F.3d 1271, 1290 (11th Cir. 2015); *Castle v. Sangamo Weston, Inc.*, 837 F.2d 1550, 1563 (11th Cir. 1988) ("The decision whether to grant equitable relief, and, if granted, what form it shall take, lies in the discretion of the district court."). "Crafting a preliminary injunction is an exercise of discretion and judgment, often dependent as much on the equities of a given case as the substance of the legal issues it presents." *Trump v. Int'l Refugee Assistance Project*, ___ U.S. ___, 137 S. Ct. 2080, 2087, 198 L.Ed.2d 643 (2017) (per curiam); *Kansas v. Nebraska*, 574 U.S. 445, 456, 135 S.Ct. 1042, 191 L.Ed.2d 1 (2015) (noting that a court of equity may "`mold each decree to the necessities of the particular case' and `accord full justice' to all parties"). In formulating the appropriate remedy, "a court need not grant the total relief sought by the applicant but may mold its decree to meet the exigencies of the particular case." *Int'l Refugee Assistance Project*, 137 S. Ct. at 2087 (citation omitted). And the Supreme Court has repeatedly advised, "[w]hen federal law is at issue and `the public interest is involved,' a federal court's `equitable powers assume an even broader and more flexible character than when only a private controversy is at stake.'" *Kansas v. Nebraska*, 574 U.S. at 456, 135 S.Ct. 1042 (citing *Porter v. Warner Holding Co.*, 328 U.S. 395, 398, 66 S.Ct. 1086, 90 L.Ed. 1332 (1946) and *Virginian R. Co. v. Railway Employees*, 300 U.S. 515, 552, 57 S.Ct. 592, 81 L.Ed. 789 (1937)).

B. Standard for Challenging Constitutionality of State Election Laws/Systems

When considering the constitutionality of an election law, the Court applies the framework established by the Supreme Court in *Anderson v. Celebrezze* and *Burdick v. Takushi*. Under this framework, referred to as the *Anderson-Burdick* test, when deciding whether a state election law violates the due process rights guaranteed by 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, 112 S.Ct. 2059, 119 1273*1273 L.Ed.2d 245 (1992); *Anderson v. Celebrezze*, 460 U.S. 780, 103 S.Ct. 1564, 75 L.Ed.2d 547 (1983). "[T]he level of the scrutiny to which election laws are subject varies with the burden they impose on constitutionally protected rights." *Stein v. Alabama Sec'y of State*, 774 F.3d 689, 694 (11th Cir. 2014). A law that severely burdens the right to vote must be narrowly drawn to serve a compelling state interest. *Burdick*, 504 U.S. at 434, 112 S.Ct. 2059; *Democratic Exec. Comm. of Florida v. Lee*, 915 F.3d 1312, 1318 (11th Cir. 2019). But "reasonable, nondiscriminatory restrictions" that impose a minimal burden may be warranted by "the State's important regulatory interests." *Common Cause/Ga. v. Billups*, 554 F.3d 1340, 1352 (11th Cir. 2009) (citing *Anderson*, 460 U.S. at 788, 103 S.Ct. 1564). "And even when a law imposes only a slight burden on the right to vote, relevant and legitimate interests of sufficient weight still must justify that burden." *Lee*, 915 F.3d at 1318-19; *Billups*, 554 F.3d at 1352.

III. Discussion of Claims and Relief Issues

A. Background Context

Georgia's new 2019 Election Code mandates that "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 and for absentee ballots cast in person, unless otherwise authorized by law; provided, however, that such electronic ballot markers shall produce paper ballots which are marked with the elector's choices in a format readable by the elector." O.C.G.A. § 21-2-300(a)(2). The legislation places the responsibility of selecting the equipment for the new voting system with the Secretary of State. *See* O.C.G.A. § 21-2-300(a). The law expressly requires that the "equipment used for casting and counting votes in county, state, and federal elections shall be the same in each county of this state and shall be *provided to each county by the state, as determined by the Secretary of State.*" O.C.G.A. § 21-2-300(a)(1) (emphasis added).

The Election Code further requires the Secretary of State to certify the new BMD voting system as "safe and practicable for use" in compliance with the Rules of the Georgia State Election Board prior to authorizing its implementation in state, federal, and county elections in the State. O.C.G.A. § 21-2-300(a)(2); *see also* Ga. Comp. R. & Reg. 590-8-1-.01(d). It also requires that the state furnished uniform electronic ballot system "be certified by the United States Election Assistance Commission prior to purchase, lease, or acquisition." O.C.G.A. § 21-2-300(a)(3). The Election Code tasks the Georgia State Election Board with promulgating rules and regulations governing audit procedures and requires that "[t]he procedures prescribed by the State Election Board shall include security procedures to ensure that collection of validly cast ballots is complete, accurate, and trustworthy throughout the audit." O.C.G.A. § 21-2-498(b)&(d).

The legislation enacted in April 2019 was adopted on the heels of a number of public events revolving around Georgia's outdated DRE election system: a widely publicized breach of the State's election server maintained by the State's election services contractor, Kennesaw State University, that exposed voluminous voter data, as well as sensitive software applications and passwords that triggered the transfer of the University's Center for Election Services election operations directly to the 1274*1274 Secretary of State's office from its contractor after December 31, 2017;[9] a prior failed effort to pass election legislation during the winter legislative session of 2018 to phase out the old DRE voting machines and State Global Election Management Systems ("GEMS") that dated back to 2001; and this Court's Order in September 2018 on the Plaintiffs' Motions for Preliminary Injunction declining to enter the injunctive relief requested but finding that the Plaintiffs had demonstrated a likelihood of prevailing on the merits of their claim that the outdated DRE system as implemented was constitutionally not sustainable.[10]

The State commenced replacement of the DRE/GEMS system with Dominion's BMD system beginning in the summer of 2019 after conclusion of the request for proposals and contracting processes. This voting system change, targeted for completion in time for full implementation in 2020, was a major shift and undertaking. Dominion plays a large role in all dimensions of the implementation of the new voting system in partnership with the Secretary of State's Office.[11] The contract was entered at a time when the cybersecurity risks and vulnerabilities of digital election systems had emerged as a major concern of national leadership and as well as prominent computer engineering and cybersecurity experts and academic organizations. Election

systems were now classified as critical national infrastructure. Voter-verified ballots and hand-marked ballots in particular were deemed important tools for protecting the security of voting systems by leaders in the academic cybersecurity field, including the sole information technology and cybersecurity expert on the Commission[12] appointed by the Secretary of the State to provide recommendations regarding the replacement of the DRE System. (*See* August 15, 2019 Order, Doc. 579 at 35-42; September 17, 2018 Order, Doc. 309 at 11-12.)

Georgia is the only state using the Dominion barcode-based BMD system statewide as the mandatory voting method for all in-person voters. (*See* Decl. of Dr. Eric Coomer, Doc. 658-2 ¶ 5) ("Dominion's ImageCast X BMD system is currently used by Cook County and the City of Chicago, Illinois, several jurisdictions within the States of Michigan and Pennsylvania, and will be used by several California counties including San Francisco, Alameda, Riverside, Contra Costa, and San Diego in the upcoming 2020 election cycle."). According 1275*1275 to a study by Verified Voting, Georgia and South Carolina[13] are the only states that require the use of BMDs as the primary method for all voters. (Decl. of Warren Stewart,[14] Doc. 681-2; Decl. of Dr. Alex Halderman, Doc. 785-2 ¶ 47; Decl. of Dr. Alex Halderman, Doc. 855-1 at ¶ 3.) The majority of election jurisdictions across the U.S. use hand-marked paper ballots as the primary method of voting and provide BMDs exclusively for voters who request them for accessibility (e.g., those with certain disabilities) or upon voter request.[15]

The Secretary of State's Office contracted with Dominion for all equipment and software components of the system (the BMD touchscreens, attached ballot printers, ImageCast optical scanners that tabulate ballot votes, and the KnowInk Poll-Pads) but continued to use its ENET voter registration database system. The ENET system provides the voter data foundation for the PollPads used for voter check-in at the polls.

In entering into the Dominion contract, the Secretary of State proceeded with an agreement for the current level of capacity of Dominion's ImageCast optical scanner to tabulate votes based on the scanned image of the QR barcode encoded with the voter's designated ballot selections. The Dominion ImageCast optical scanners used by Georgia in tandem with the BMDs are capable of scanning and tabulating votes without a QR barcode. (Decl. of Dr. Eric Coomer, Doc. 658-2 ¶ 9; Decl. of Dr. Alex Halderman, Doc. 785-2 ¶¶ 4, 37-40.) In response to the State's request for proposals during the procurement process, Dominion represented that an upcoming version of its BMD software would not need to print barcodes on ballots.[16] The BMDs under the prospective option would instead produce a human-readable ballot that would be counted by the optical scanner/tabulators based on voters' electronic vote designations on the ballot by reading particular target areas associated with the voter selections, similar to how they are programmed to read hand-marked paper ballots. (Decl. of Dr. Eric Coomer, Doc. 658-2 ¶ 9; Decl. of Dr. Alex Halderman, Doc. 785-2 ¶ 37.) This option is described as an "upgrade" available only after "certification is complete at the EAC."[17] The Court assumes that cost considerations, among others, may have played a role in this purchasing decision, as it was currently available through some other vendors.[18] However, the State's actual option in the long run of upgrading the system to one that tabulates from the voter designations, and not a QR barcode is potentially relevant.[19] When that might occur is another 1276*1276 question, as the EAC has apparently yet to certify Dominion's upgrade option, and in any event, it may entail costs the State might not be willing to incur.

The Court focuses in this Order on the salient evidence that Plaintiffs have presented in support of their Motions to demonstrate the constitutional infirmity of the system because of its alleged impact on voters' exercise of the right to vote and whether their votes will be counted as cast or at all.

The Court recognizes from the outset that the State Defendants did face significant challenges in implementing a new statewide voting system in barely 15 months and that early elections and primaries would occur prior to the ultimate election date of November 3, 2020. The Covid-19 pandemic further complicated that challenge. While this fact does not in any way erase the issues raised by Plaintiffs, especially in the context of the particular record in this case, the Court still bears this pragmatic reality in mind.

The Court divides its discussion below of the motions before it as follows. Section B addresses the evidence presented in conjunction with the Curling Plaintiffs' Motion for Preliminary Injunction and a portion of the Coalition Plaintiffs' Motion for Preliminary Injunction on BMDs, Scanners and Tabulators and Audits. Section C addresses the Coalition Plaintiffs' Motion related to the issue of ballot secrecy. Section D addresses that portion of the Coalition's Motion as to Scanners and Tabulators focused on the review and counting of hand-marked ballots, including absentee ballots, provisional ballots, and finally, some portion of emergency ballots cast.[20]

B. Claims Relating to BMDs, Scanners/Tabulators, and Audits

1. Cybersecurity Risks and Reliability Issues Presented by Implementation of the BMD System

The evidence, expert opinion testimony, and argument Plaintiffs offer in support of their challenge to the constitutionality of the State Defendants' implementation of a barcode-based system for all in-person voting falls into three main areas. They contend that the evidence shows:

(1) The QR barcode-based BMD voting system does not produce a voter-verifiable paper record of the votes cast. Therefore, voters will be unable to conduct any verification of the information encoded in the non-human readable barcode, will have no way of knowing what votes they are actually casting, and will instead be forced to trust that the barcode accurately conveys their intended ballot selections. Both the QR barcode recording of votes and the text summary of ballot selections are subject to being accessed and manipulated through hacking, unauthorized intrusion into the BMD computer system or its various components (scanner, printer, etc.), by USB flash drives (or similar devices), or by other interfaces with the internet through cyber attacks or applications that may be carrying malware (whether intentionally or not).

1277*1277 (2) The QR barcode-based BMD voting system poses major security and fidelity of vote issues because the BMD system is susceptible to significant cybersecurity risks and manipulation through hacking access to any one of its multiple components (BMD, printer, scanner) and through untraceable manipulation or alteration of code. The QR barcode is not encrypted and may also be a vector of data system manipulation.

(3) The QR barcode-based BMD voting system is incapable of being meaningfully audited for a variety of reasons: (a) the QR code cannot itself be verified by a voter; (b) the length and complexity of many ballots and the printed ballot text's condensed mode of summarizing the voter's ballot selections (identifying solely the candidate selected by office or condensed constitutional amendment summaries identified by question number or by a few words); and (c) research reflecting that most voters do not review these printed ballot summaries, and those that do, will not detect errors in ballots presented for verification based solely on their memories.

Plaintiffs presented multiple expert witnesses to address their assessment of the Dominion system's cyber risk vulnerabilities and incapacity to provide a voter verifiable or auditable vote.[21] Plaintiffs' experts testifying at the hearing or by affidavit included: Dr. Andrew W. Appel, Dr. Richard DeMillo, Dr. J. Alex Halderman, Mr. Harri Hursti, Mr. Vincent Liu, Mr. Kevin Skoglund, and Dr. Philip B. Stark.

Defendants have contested Plaintiffs' cybersecurity, vote fidelity, and voting system evidence through cross-examination as well as through the testimony of the State's witnesses and Dr. Eric Coomer, Director of Product Strategy and Security for Dominion Voting Systems, and the testimony of Jack Cobb, the Director of Pro V&V, the United States EAC accredited private laboratory retained by the Georgia Secretary of State to assess and test Dominion's Democracy Suite 5.5-A voting system software and associated components[22] and the KnowInk electronic pollbook as deployed in Georgia for EAC certification. Although Mr. Cobb's affidavits addressed cybersecurity related matters, his testimony at the injunction hearing plainly indicated that he actually claims no specialized knowledge or background in cybersecurity engineering and did not himself perform any security risk analysis of the BMD system. Defendants did not introduce any evidence from Fortalice Solutions, the cybersecurity consulting firm that previously has performed security 1278*1278 analysis regarding the Secretary of State's information technology system, as discussed in the Court's Order of August 15, 2019 and which conducted a confidential initial evaluation of the BMD system in November 2019 at Defendants' counsel's request on behalf of the Secretary of State. Thus, the State Defendants did not present any independent cybersecurity expert to directly address the cybersecurity issues and risk vulnerabilities of Dominions' QR code voting system raised by Plaintiffs. Instead, State Defendants relied on Dr. Coomer's testimony, to address — based on his professional experience[23] — some of the significant cybersecurity issues raised by Plaintiffs. The State Defendants also provided expert testimony regarding the issue of whether a QR code based voting system, where votes are recorded and tabulated based on a scanner/tabulator's reading of the QR code, can be properly subject to a risk-limiting audit as to the outcome of any specific election in response to the extensive testimony provided by Plaintiffs' experts on this subject.

Plaintiffs' substantive evidence regarding the Defendants' implementation or usage of the BMDs, scanner/tabulators, and audits is the most complex, expert-intense evidence presented in this case. Indeed, this array of experts and subject matter specialists provided a huge volume of significant evidence regarding the security risks and deficits in the system as implemented both in witness declarations and live testimony at the preliminary injunction hearing.[24] As authorized discovery only commenced shortly before the preliminary injunction hearing, no expert or other depositions had been conducted.

While Plaintiffs' experts provided illuminating evidence, this evidence still had its own constraints. *First,* security information from the Secretary of State's office was limited. The Secretary of State's response to Plaintiffs' authorized expedited discovery requests indicated that its cybersecurity consultant, Fortalice Solutions, had not generated any consulting studies, audits, or assessments of data system security issues since August 1, 2019 when the State commenced its early work on implementation of the Dominion system, other than a November 2019 report requested by Defendants' counsel and withheld based on attorney work product privilege.[25] (*See* September 2, 2020 Order, Doc. 858 (approving non-disclosure based on assertion of privilege and in turn, granting on limited terms Plaintiffs' request for inspection 1279*1279 of BMD equipment); *see also,* August 15, 2019 Order, Doc. 579 at 73-90 (discussing the focus of Fortalice evaluations of security and software issues prior to August 2019).) *Second,* while some of Plaintiffs' experts had accessed other related BMD models and Dominion software previously, the specific BMD model and software variation (along with the optical scanners/tabulators programmed with Dominion's proprietary software) used in Georgia was not accessible to the Plaintiffs and their cybersecurity expert, Dr. Halderman, until Friday, September 4, 2020 at 5:30 p.m. — and then, only by Court Order.[26] This was just days before the preliminary injunction hearing commenced on September 10, 2020. Upon the Plaintiffs' filing of a discovery dispute notice regarding their access issue, the Court ordered the swift production of a BMD and related ImageCast precinct scanner for Plaintiffs' expert's testing and assessment, subject to various confidentiality provisions and other terms.[27] (As the Dominion system uses an off-the-shelf printer, the Plaintiffs provided their own new printer of the same model used by the Defendants.)

Dr. Halderman's testing of the equipment and software occurred over the short period of time before the scheduled hearing.[28] His evaluation in this abbreviated time frame yielded some supplemental results that supported the Plaintiffs' cybersecurity analysis of the malware vulnerability risks of this specific BMD system. In particular, Dr. Halderman's testing indicated the practical feasibility through a cyber attack of causing the swapping or deletion of specific votes cast and the compromise of the system through different cyber attack strategies, including through access to and alteration or manipulation of the QR barcode.[29] As the National Academies of Sciences, Engineering, and Medicine, found in its seminal report, Securing the Vote: Protecting American Democracy 42, 80 (National Academies Press, 2018)("National Academies Report" or "NAS Report"):

[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.

(Doc. 285-1, Ex. 1.)

Dr. Halderman had physical access to the BMD system when conducting his 1280*1280 tests, which expedited his experimentation and intrusion into the software system. Evidence presented in this case overall indicates the possibility generally of hacking or malware attacks occurring in

voting systems and this particular system through a variety of routes — whether through physical access and use of a USB flash drive or another form of mini-computer, or connection with the internet. As discussed in the declarations and testimony of the proffered national cybersecurity experts in this case, a broad consensus now exists among the nation's cybersecurity experts recognizing the capacity for the unobserved injection of malware into computer systems to circumvent and access key codes and hash values to generate fraudulent codes and data. In these experts' views, these risk issues are in play in the operation of Dominion's Democracy Suite 5.5-A GA, and take on greater significance because the system is one that does not provide a verifiable and auditable ballot record because it relies on the QR code for vote tabulation and that code itself cannot be read and verified by the voter. (*See, e.g.*, Declaration of Vincent Liu, Doc. 855-2 at 6-8; Tr. Vol. II at 59, 64; Declaration of Dr. Andrew Appel, Doc. 855-3 at 6; Declarations of Dr. Alex Halderman, Doc. 682 at 4-11, Doc. 785-2; *see also* Appel, A.W., R. DeMillo, and P.B. Stark,[30] Ballot-Marking Devices Cannot Ensure the Will of the Voters, Election Law Journal (2020), Doc. 619-10.) Hacking alterations of the barcodes and/or predicate text, security keys, or hash values renders tracing or auditing of the fraudulent change in voting data difficult or impossible in their viewpoint — and in turn impacts the capacity to conduct appropriate auditing of ballot data or to implement corrective "re-count" measures.

Dr. Halderman's empirical evaluation of the Georgia programmed BMD voting equipment and software was partial and incomplete due to the short time allocated for the examination prior to the injunction hearing. And Dr. Halderman indicated that he would need more time with the equipment and software to conduct further testing of the software and modeling of other malware that could attack any component of the BMD system and infect the system and recording of votes or cause other mayhem. Dr. Halderman provided directly relevant information to a demonstration of the risks facing this specific voting system. However, his evaluation and testing of the system was limited as described and not fully subject to being itself examined in depth by Dominion's own cyber security staff given the last moment nature of the testing.[31]

1281*1281 That said, Dr. Halderman has also offered other core relevant testimony in this case in open and sealed hearings as well as in sworn declarations. (*See, e.g.*, Doc. 785-2.) He as well as other cybersecurity experts testifying on behalf of Plaintiffs here have provided evidence credibly explaining how malware can mask itself when inserted in voting software systems or QR codes, erase the malware's tracks, alter data, or create system disruption. And while some attacks can be detected, their results often are not susceptible to full correction. For all these reasons, Dr. Halderman and Plaintiffs' other cybersecurity expert witnesses testified that heightened proactive protection measures are needed beyond what the current Dominion system as implemented in Georgia provides[32] or alternatively, are simply not feasible given the 1282*1282 system's central reliance on a humanly unverifiable QR code.

Plaintiffs' voluminous expert testimony describes an interrelated range of systemic software and operational practices that define and impact the functioning of the voting system. The Plaintiffs maintain that the BMD system and software design as well State Defendants' identified practices independently and as a whole undermine the integrity, security, and functionality of the voting system and in turn, adversely impact whether citizens' votes will be counted as intended or counted at all. The Court has considered this challenge on its merits because a voting system, procedure, or practice can in reality subvert or impair citizens' exercise of the franchise and the

counting of their votes. Still, the Court notes from the outset that the voting system challenged here is a new system for Georgia,[33] replacing the outdated DRE system that was dependent on totally obsolete software and defective usage practices that patently made it unreliable. Whatever the new BMD system's flaws in design, age, and reliability of components, or implementation — some of which may be significant — the evidence would at this early point in time have to be highly compelling to justify the Court's considering enjoining on a wholesale basis the State's use of the a BMD voting system approved by the Secretary of State, pursuant to his authority under a state law enacted as recently as 2019.

The issues and alleged practices identified by Plaintiffs as a basis for enjoining the system include:

• the BMD QR code's lack of encryption, that opens voting data up to breach, alteration, and other security weaknesses;
• cybersecurity risk management and practices that allegedly render the voting system vulnerable to compromise and breach, and alteration or loss of votes;
• alleged major shortcuts taken in state protocols now used for conducting Logic and Accuracy testing ("L & A") of voting machines required under Georgia law preceding each election, even though L & A testing constitutes a fundamental threshold standard to verify the correct functioning and accurate output of the BMD system and its component parts;
• the alleged impossibility or inadequacy of using Risk-Limiting Audit methodology meaningfully to audit BMD ballots and votes tallied based on a scanned QR code, where evidence indicates that only a fraction of voters review their printed ballot;
• scanning software, practices, and settings that allegedly result in voters' ballot selections on paper ballots (whether cast as absentee, provisional, or emergency ballots) being interpreted as blank and not counted, though clearly appearing on the hand-marked ballots cast by voters;
• the alleged failure to protect the confidentiality of the voting process by the use of timestamps on scanners that trace back to the voters at the precinct and by the large BMD screens that expose the voter's selection choices to other individuals in the precinct and burdening their free exercise of the franchise.

1283*1283 **2. Encryption & Risk Exposure**

The Court at some length described in its August 15, 2019 Order the changed landscape of cybersecurity in which election systems operate. More evidence emerging in the past year has added to this picture of heightened security concerns. The Court does not further delve into this reality here because the Defendants do not appear to actually dispute that cybersecurity risks are significant in the electoral sphere. Dr. Halderman's voting machine testing exercise in the 2020 preliminary injunction hearing — as in 2019 — showed how this might play out. As several of Plaintiffs' national cybersecurity and engineering experts explained in their testimony, the issues presented for any cyber electoral system is how to fortify the system's protection against unauthorized intrusion or accessing of software and databases, the system's detection and limitation of the impact of malware, and minimization of risk overall, including through active auditing procedures.[34]

The State Defendants presented the BMD system's cybersecurity as reliable and fortified both based on the testimony of Dr. Coomer as Dominion's Director of Product Strategy and Security

and the testimony of Mr. Jack Cobb, the Laboratory Director for Pro V&V.[35] The Secretary of State retained Pro V&V to perform a review of its newly adopted BMD voting system, as required for EAC certification purposes, for submission to the EAC for approval. Pro V&V originally certified the Dominion Democracy Voting's Democracy Suite 5.5-A system in August 2019 and has certified a modified version since that time — once in November 26, 2019 and once on October 2, 2020.[36] Mr. Cobb represented in his affidavits filed by Defendants that the Dominion system's security was fortified by the encryption of the QR code and accompanying digital signature code as well as various other security measures such as use of a built in security feature that generates SHA-256 hash values. (Doc. 821-6 at 4.)

Mr. Cobb testified at the injunction hearing that he had fourteen years of experience in testing voting machines, but as became apparent in the course of these proceedings, he does not have any specialized expertise in cybersecurity testing or analysis or cybersecurity risk analysis. Further, Mr. Cobb had not personally done any of the security testing referenced in his affidavits.

In his first affidavit, Mr. Cobb stated that the BMD printed ballot's QR codes are signed and encrypted. (Doc. 821-6 at 4.) When Plaintiffs' experts disputed this encryption claim, Mr. Cobb in his second affidavit pointed to Dominion's own documentation as the source of his prior statement 1284*1284 that the encoded QR codes and digital signature were encrypted.[37] And at the injunction hearing, Mr. Cobb conceded that he accepted such representations on face value rather than on any testing that he had actually done. (Tr. Vol. II at 243.) The evidence plainly contradicts any contention that the QR codes or digital signatures are encrypted here, as ultimately conceded by Mr. Cobb and expressly acknowledged later by Dr. Coomer during his testimony. (Tr. Vol. II at 123, 146, 237, 243.) In his second affidavit, Mr. Cobb averred that his prior description of the QR code as encrypted as opposed to "encoded" was just a difference in verbiage because he is not an academic. As discussed later below in connection with Mr. Vincent Liu's testimony, this is simply not correct. Similarly, during cross examination, after conceding that malware could affect hash value generation, Mr. Cobb indicated he was not familiar with the fact that malware could defeat or disable the hash values[38] — a concern addressed by all of Plaintiffs' cybersecurity specialists who provided declarations or testimony in this case.

Mr. Cobb's first affidavit discloses that Pro V&V did not itself conduct any form of penetration or security testing of the 5.5-A software version specifically to be used in Georgia (certified by Dominion in August 2019) but relied on another company's security testing of earlier versions of the Dominion Democracy Suite software.[39] (Doc. 865-1 at 5; Tr. Vol. II, at 233.)[40] Dr. Coomer testified that there is a difference between the 5.5 and 5.5-A Dominion Democracy Suite versions — a change to the ICX software that was not deemed de minimis. (Tr. Vol. II at 138.) Pro V&V's assessment of the modified software version in November 2019 ("5.5.A GA" update) (classified as de minimis) was performed by an employee no longer with the company. Mr. Cobb's affidavit did not indicate that he actually had personal familiarity with that specific testing or actually any specific testing, as he testified he did not engage in this type of activity. (Tr. Vol. II at 243.) At the injunction hearing, he indicated that Pro V&V had never tried or tested alteration of the QR code in Dominion version 5.5-A, though he had previously declared in effect that this could not be done. (Tr. Vol. II at 238.) While Mr. Cobb's affidavits addressed cybersecurity matters and criticisms of Plaintiffs' cybersecurity and engineering expert affidavits,

he was candid in his testimony at the injunction hearing that he actually had no specific expertise in cybersecurity testing.

Mr. Vincent Liu, is a leading international cybersecurity analyst and consultant. He has focused on the "offensive side of security for 21 years," starting with the National Security Agency as a global network exploitation analyst and moving from there to work at Ernst & Young in their advanced security centers. He subsequently led the global penetration team for 1285*1285 Honeywell International and in 2005 co-founded the cybersecurity firm of Bishop Fox of which he is CEO. As he describes, "we are hired by some of the most sophisticated, largest companies in the world to perform product security testing, application security testing, penetration testing, code reviews, red teaming. Essentially, companies hire us to find vulnerabilities within their system to identify weaknesses."[41] (Liu Testimony, Tr. Vol. II at 54.)

Mr. Liu addressed head-on the inaccuracy of any contention that the QR code or signature utilized in the Dominion BMD system in Georgia is encrypted. Mr. Liu testified at the injunction hearing that based on his and his firm's examination of the QR codes, the codes were not encrypted. "And the process that we undertook to perform the verification was to develop code that read the QR code. Wherein, we were able to extract the raw data and determine ... whether or not it was encrypted. And our conclusion was that it was not." (Liu Testimony, Vol. II at 56.) Mr. Liu further explained that encryption and encoding have fundamentally different meanings. "The use of encryption implies that there is an algorithm that confers some measure of security to the system.... [A] way to think about it is encryption is used to provide security. Encoding is intended for usability. It is to make information more easily accessible, which is oftentimes counter to, say, encryption, which is something more secret .... [I]t is a concept that is very, very fundamental." (*Id.* at 57.) QR codes, in short, are made to facilitate access, not to conceal the code.

Mr. Liu also addressed whether the digital signature in the Dominion QR code provided security for the QR code:

[T]ypically when you are thinking about digital signatures you are referring to the use of public-key cryptography. And the intention is to provide for integrity. In this case, public-key cryptography was not being used with QR codes. And so the implication is that with the BMDs and the generation of the QR codes the QR codes themselves — the implication with the design of the Dominion BMD system is that any device that has necessary keys to operate would be able to generate a fake QR code. And you would not be able to determine which machine generated it, whether it was the EMS, the BMD, the ICP, or any other system that had that key loaded on to it.

(*Id.* at 58.)

Mr. Liu goes on to dismiss Pro V&V's and Dominion's reliance on hash values as a central software security protective device. "[I]f you have an infected BMD that has been compromised [by malware], it can just tell you whatever value that it wants." (*Id.* at 59.) "[A]s it is deployed within the Dominion devices, it does not appear to be used in a fashion that could be considered secure. It can easily be circumvented." (*Id.* at 64.) Liu similarly addresses the insecurity of the

encryption key and other gateways to the system that he states can be bypassed by malware to allow access to QR codes (and faking of such). (*Id.* at 60-61, 63; Liu Decl., Doc. 855-2 at 5-8.)

On cross-examination, Mr. Liu explained that while he had not personally physically examined the BMD system in Georgia because 1286*1286 it has not been accessible for independent evaluation, he had used established standard cybersecurity evaluation practices for assessing the vulnerability of software. Liu reviewed the architecture and documentation regarding this specific BMD system (including certification documentation) and considered the outdated Android operating system[42] and principles of how relevant checksum software works, his knowledge of applicable technology and software principles and cybersecurity vulnerabilities. (*Id.* at 63-67.) He also considered the system's use of USB devices and portals which in his view generally are "fraught with security concerns." (*Id.* at 69-70.) Liu concluded that in his view, the design of the security of the BMD system is not secure and "require[s] a more in-depth review." (*Id.* at 68.)

In contrast, Defendants contend that Plaintiffs' evidence boils down to hypothetical speculation by Dr. Halderman about what "could" happen based on his experience with other electronic voter systems, and review of Dominion documentation, rather than a studied evaluation of the Dominion 5.5-A GA system or its implementation. They argue that the Plaintiffs' experts have never actually seen malware that would actually alter a ballot on the Dominion voting system. The State Defendants also question Dr. Halderman's mode of testing the BMD system when the Court ordered the equipment be made available for confidential testing in early September[43] and assessment of the vulnerability of the system's design.

Given the Court's assessment of the limitations in Mr. Cobbs' and Pro V&V's evaluation of cybersecurity elements of Georgia's BMD system and affidavit accuracy issues, the Court looks to Dr. Coomer's testimony for a fuller picture. Dr. Coomer averred in his November 2019 affidavit, "while all computers can be hacked with enough time and access, Dominion is not aware of any situation where an individual used the barcode on one of its units to launch software or to affect the operation of the unit." (Doc. 852-1 at 8.) In his court testimony, Dr. Coomer describes Dominion's Democracy Suite system as a protected "end-to-end" election management system that is a "self-contained, self-functioning election management system and tallying tabulation system." (Tr. Vol. II at 117.)

Dr. Coomer represents that the servers and work-stations are "hardened" to meet benchmarks set by NIST, the National Institute of Standards Technology. And he represented to the Court that the NIST benchmarks do not address whether other software applications — i.e., game applications that Mr. Hursti observed on servers in Georgia county voting offices — must be removed to ensure that servers are securely hardened and protected.[44] Dr. Coomer testified that one of the strong assets of 1287*1287 the system's touchscreen interface is that voters cannot cast overvotes (more than one vote in a single race) and that undervotes (no vote cast) are clearly indicated to the voter on the screen, thereby addressing "a lot of the voter intent issues you have with hand-marked ballots." (*Id.* at 119.) And in this connection, he commented on the clarity of the touchscreens that do not have the calibration problems posed by legacy voting systems. (*Id.* at 121.)

Dr. Coomer testified at the injunction hearing that Dominion did not intend to encrypt the QR barcode. He also testified regarding the use of digital signatures, secure keys in the system "that are part of the system and the standard SHA-256 hashing algorithm" as protective security architecture for the software system and the QR codes.[45] (Tr. Vol. II at 123.) Responding to State Defendants' question regarding what would be necessary to generate a valid (but false) QR code accepted by the ICP scanner, Dr. Coomer discussed how *all* physical and software defenses of the system would have to be defeated and source code accessed, which his testimony as a whole suggests he did not think likely. (Tr. Vol. II. at 124.) He also in his 2019 affidavit testified that as the BMD touch-screen tablets run the Dominion Voting Systems software in Kiosk mode (in a mode only showing the Touchscreen voting display), "this prevents any access to software or features outside of the certified installed program." (Doc. 821-1 at 2-3.) Finally, Dr. Coomer's affidavit represents that "the BMD has no physical component that would allow for wireless transmissions."[46] (Id.) Dr. Coomer acknowledged on cross examination, however, that the Democracy Suite software works on an Android operating system that is separate from the software and hardware, and that is not written by Dominion. (Tr. Vol. II at 86-87.) He further acknowledged the potential for compromise of the operating system, by exploiting a vulnerability, that could allow a hacker to take over the voting machine and compromise the security of the voting system software. (*Id.*)

The evidence of actual implementation presented by Harri Hursti's testimony suggest a very different picture as to the system's implementation at this juncture. Mr. Hursti is a nationally recognized cybersecurity expert who has worked in security-oriented IT technology for over 30 years, with a particular expertise in the knowledge, observation and prevention of malicious activities in networked environments. Mr. Hursti also has an expertise in optical scanning. (Doc. 680-1 at 37; Doc. 853-2; Tr. Vol. I at 120-121.) Mr. Hursti is the co-founder and organizer of one of the largest annual cybersecurity and hacker community meetings, attracting over 30,000 participants in Las Vegas in the four years prior to the Covid-19 pandemic. He also organized the 2018 Voting Machine Hacking Village for which he was awarded a Cyber Security Excellence Award and has engaged in other organized efforts to work with local election officials to assist them in gaining security expertise.

In response to the State Defendants' critique of his specific qualifications, Mr. Hursti indicates that "there are only a few independent voting system researchers with more hands-on experience than I 1288*1288 have with key components of the Dominion Voting System elements. To my knowledge, no jurisdiction has permitted, and Dominion has not permitted, independent research, academic or otherwise, to be conducted on its systems, which greatly limits the number of people with any experience with the Dominion systems." (Doc. 853-2 at 2.) He notes that the Voting Machine Hacking Village issued its 2019 annual report that addressed security weaknesses, vulnerability, and exploitations discovered by the participants regarding an array of computing systems, including a different hybrid piece of Dominion voting equipment, the ImageCast Precinct with Ballot-Marking Device.[47] (*Id.* at 3.) The report intentionally did not provide a public disclosure of how the exploits were conducted but instead a high-level overview. Hursti states that he was actively engaged with the underlying work and that the discoveries were intentionally not included in the annual report for protective security reasons. He has evaluated BMD-type devices during the DEF CON conference and otherwise. He has

also conducted in-person observations of electoral operations and scanning in Georgia precincts and county offices during the last year since the introduction of Dominion's BMD system.

Mr. Hursti testified at the September 2020 injunction hearing and through several declarations regarding his observations made while visiting county facilities where voting activity was transpiring in the August 2020 elections and in other sites both before and after the August observations. Based on his cybersecurity expertise and in-depth knowledge hacker strategies, Hursti identified concerns regarding the security of these systems. He found that in the two county election offices he visited, election servers enabled unsafe remote access to the system through a variety of means, extending from frequent use of flash drives and accessing of the internet to the use of outside unauthorized applications (such as game programs) residing on election management and tabulation servers and other practices. Mr. Hursti testified that these practices drive a hole through the essential cybersecurity foundation requirement of maintaining a "hardened"[48] server (and associated computers) 1289*1289 as well as air gapped secure protection of the system. Without these basic protections, malware can far more easily penetrate the server and the operative BMD system software in turn.

Hursti found that in one of the counties, server logs were not regularly recording or updated in full and that Dominion's technical staff maintained control over the logs and made deletions in portions of the logs. Yet secure and complete logs, Hursti testified, are essential as the most basic feature of system security as they provide the detailed activity trail necessary for the identification of security threats and server activity and are required for purposes of conducting a sound audit.[49] (*See* Hursti Decl., Doc. 853-2; Tr. Vol. II at 117-169.)

In sum, at the preliminary injunction hearing, Mr. Hursti succinctly presented his opinion that given the irregularities that he observed as a cybersecurity expert he had serious doubt that the system was operating correctly and that "when you don't have an end-to-end chain of the voter's intent" and when a system could be maliciously or unintentionally compromised, there is no capability of auditing the system results.

3. Other Issues: Software Changes and Installation

In addition to the above issues, approximately two weeks after the last day of the injunction hearing in this case, a new development or crisis (depending on which party's perspective) was brought to the Court's attention. Logic and Accuracy testing in at least two counties demonstrated an unpredictable defect or bug in the presentation on the ballot of the 20 candidates for one of Georgia's U.S. Senate seats. A column of the senatorial candidates erratically would disappear from the ballot. Dominion conducted expedited testing to identify the source of the bug. At first it determined it would have to replace the database system wide across Georgia to address the issue. On the afternoon of September 25, 2020, Chris Harvey, the Director of Elections for the Secretary of State's Office, issued a written notice to all County election directors regarding a ballot problem that had arisen that might require replacement of the entire voting database. He therefore directed that all county election offices cease Logic & Accuracy testing until further notice. Georgia's 159 counties thus temporarily halted all Logic and Accuracy testing preparation of voting equipment for the elections.

Plaintiffs' counsel notified the Court over the ensuing weekend of this significant new election system problem. The Court held a phone conference with counsel along with Dr. Coomer regarding the issues raised on September 28th. The Court was at that time advised that Dominion had now determined after further testing that the issue should be addressed by a software modification to run on the ICX BMD Touchscreen voting machines that would have to be installed in each of these BMD voting machines across the state. Meanwhile, Dominion sent a modified version of the software for running the election on the operative ICX BMD Touchscreen voting equipment to Pro V&V for 1290*1290 independent testing.1 Although as it turns out, Pro V&V had not started their testing of the software modification (or so it seems) aimed at remedying the issue at the time of the September 28th phone call, Dr. Coomer initially advised the Court then that "so the testing lab has already deemed the change de minimis" — an instantaneous conclusion that bears consequences and raises questions, as later discussed here. (Tr., Sept. 28, 2020, Doc. 926 at 38.) Dr. Coomer then responded to the Court's question of when therefore did the testing actually occur. He further responded that Pro V&V had first analyzed the code change to determine if the change was "de minimis" pursuant to EAC standards and then, based on that finding, would conduct testing, which was proceeding on that day, Monday, September 28th.[50] By Tuesday at latest, Pro V&V had given its full approval of the software modification, though it had yet to issue a written testing report. By that Tuesday afternoon or evening (or earlier), Pro V&V had transmitted the modified software to the State Elections Division for review, use, and distribution to counties on Wednesday. (Doc. 928-1.) The State in turn transmitted on Wednesday, September 30th one flash drive to each county elections office for mass reproduction in hundreds of flash drives for installation of replacement software on all BMDs.

At the time it was distributed to the counties, the Dominion software modification had not yet been reviewed or approved by the Election Assistance Commission.[51] The State contends it could immediately legally proceed without such approval and has now launched and apparently completed the process of Counties' (whether by county staff or Dominion staff or contract employees) removal of the prior software and installation of the new modified software in thousands of voting machines across the state. At conferences held by the Court on September 28th and October 1st, the State Defendants' counsel maintained that the State did not need EAC approval to implement newly modified software essential to running all critical aspects of the voting machines as state law only requires that the BMD system be "certified by the United States Election Assistance Commission prior to purchase, lease, or acquisition." O.C.G.A. § 21-2-300(a)(3). (Tr. of Sept. 28, 2020 hearing, Doc. 925.) The State Defendants filed at the Court's directive the Pro V&V written testing documentation on October 2, 2020 and represented in the same filing that the Pro V&V summary letter had been submitted to the EAC. However, Dominion did not in fact submit the software modification for approval to the EAC as a de minimis change until Monday, October 5, 2020 and then re-submitted 1291*1291 its engineering change order request on Tuesday evening, October 6, 2020, a day after installation of new software statewide in BMDs across the state's 159 counties was completed.[52] (Doc. 959-5.) And on Wednesday, October 7, 2020, upon the EAC's request, Pro V&V submitted the engineering change order to the EAC verifying that it viewed the software change as de minimis and did not require further testing. (Doc. 959-5 at 11.) The EAC notified Dominion of its approval on Friday, October 9, 2020 in a one-line sentence. (Doc. 960-1.) The Court is certainly not in the position to second guess the EAC's approval. But it does delineate here the entire sequence of events and

review to make transparent that the EAC review process and associated independent private laboratory review process does not offer exactly a firm protective shield as the EAC functions on a voluntary cooperation basis and does not exercise independent regulatory authority.

EAC Certification requirements specify that pre-approval of software program modifications is necessary, even if considered "de minimis" because of the potential systemic impacts of software changes. Section 3.4.3 of the EAC Certification Manual (revised November 19, 2019) provides: "Manufacturers who wish to implement a proposed de minimis change must submit it for VSTL review and EAC approval. A proposed de minimis change may not be implemented as such until it has been approved in writing by the EAC." The EAC Manual regulatory revision at 3.4.3.1. (3) specifies that a Voting System Test Laboratory (VSTL) (in this case, Pro V&V) must review and assess the proposed change and among other requirements, detail "the basis for its determination that the change will not alter the system's reliability, functionality, or operation." It also must determine whether the change meets the definition or instead "requires the voting system to undergo additional testing as a system modification." Section 3.4.3.1(7). In turn, if the VSTL endorses the proposed change as de minimis and provides requisite documentation, EAC "has sole authority to determine whether the VSTL endorsed change constitutes a de minimis change under this section." Section 3.4.3.3. If the EAC determines that the proposed de minimis change cannot be approved, "the proposed change will be considered a modification and require testing and certification" consistent with the requirements of the EAC manual. The Manual provision goes on to delineate six types of features of a proposed software change that should be reviewed in determining whether a change is de minimis or a modification that requires more testing.

The Plaintiffs maintain that the software changes are far more than de minimis and can have broad systemic impact. Three of their cybersecurity experts submitted affidavits regarding the issues raised by the new software and its testing, thus far. The Plaintiffs' experts' affidavits address the EAC delineated characteristics for determining if a software change is de minimis and conclude that the VSTL (Pro V&V) failed to implement requisite testing measures and analysis to determine the impact of the proposed software code changes on overall system software functionality, as required for assessment of whether a software change is "de minimis." They further contend that Pro V&V conducted a rubberstamp highly abbreviated testing review of the software changes that failed to test the 1292*1292 software changes properly to determine (a) the source of the bug or that the software modification actually fixed the actual source of the bug or (b) how or if the new modified code included in the software would impact the structure and function of other code in the software or functionality of the software as a whole. (Pro V&V Testing Report, Doc. 939; Declarations of Dr. Halderman and Kevin Skoglund, Docs. 941, 943.)

Other substantive concerns were also raised in Plaintiffs' experts' affidavits regarding the nature of the Pro V&V testing, review, and issues posed by the software change. Pro V&V reproduced the bug on a mock election panel database it had created and ran Dominion's new software version on that sample to determine the bug did not reappear. However, as Pro V&V was never able to reproduce the flickering on/off appearance of one column of the 20 candidate screen on a copy of Douglas' County's actual database that first demonstrated the bug, there is no indication that Pro V&V actually identified the root cause of the bug or that Pro V&V actually verified that the new software fixed the bug or fixed it without impacting other portions of the software. Finally, Plaintiffs' two experts discuss how in their experience, rushed, last minute software code

changes without assessment of their impact on the functionality of software and code as a whole constitutes an enormous functionality and security risk for the election system.[53] Mr. Skoglund additionally states that Logic and Accuracy testing, that should follow the new software installation process in every county, will not be able to catch the range of errors and software functionality problems potentially created by the new software. (Skoglund Decl., Doc. 943.)

Additionally, Plaintiffs have offered an affidavit from cybersecurity expert Harri Hursti who witnessed on October 1, 2020 some of the initial installation of the software now proceeding on approximately 3,300 of Fulton County's ballot marking device touchscreen units to ICX software version 5.5.10.32 in the Fulton County Election Preparation Center. (Doc. 942.) He describes in detail how 14 Dominion technicians en masse engaged in removal of the old software and installation of the new software in disorganized, rushed, and careless form — without consistent implementation of various required steps and Dominion directives for installation of the software or any evident security standards or tracking of flash drives containing sensitive information. In Hursti's view, the entire hasty and unprofessional software swap out and installation process is itself cause for grave concern as to the future security and consistent functionality of the new system.

4. Logic and Accuracy Testing

Pre-election Logic and Accuracy Testing (L & A) is an important operations verification practice and standard in jurisdictions across the nation that use any form of computerized voting equipment. L & A testing is required under the 2019 Georgia statutory provisions enacted as part of the adoption of legislation approving the statewide usage of the BMD system. As discussed below, L & A testing is designed to 1293*1293 verify pre-election that all voting equipment, BMD touchscreens, printers, scanners, and PollPads are properly configured and functioning. L & A testing should also confirm that the voting system tabulators are accurately tabulating cast ballots going into the election. The testing gives election staff an opportunity to identify basic errors in election and ballot configuration and related vote attribution in scanning and ballot printing as well as to address other basic functionality problems.

O.C.G.A. § 21-2-379.25(c) provides:

On or before the third day preceding a primary or election, including special primaries, special elections, and referendum elections, the superintendent shall have each electronic ballot marker tested to ascertain that it will correctly record the votes cast for all offices and on all questions and produce a ballot reflecting such choices of the elector in a manner that the State Election Board shall prescribe by rule or regulation. Public notice of the time and place of the test shall be made at least five days prior thereto; provided, however, that, in the case of a runoff, the public notice shall be made at least three days prior thereto. Representatives of political parties and bodies, news media, and the public shall be permitted to observe such tests.

(Emphasis added). The language of Georgia's 2019 statutory provision appears transparent: Each County superintendent shall have each electronic ballot marker machine (i.e., BMD and its components) tested to ascertain that "it will correctly record the votes cast for all offices and on all questions and produce a ballot" for such offices. O.C.G.A. § 21-2-379.25(c) (emphasis

added). This provision was adopted simultaneous to the Legislature's enactment of O.C.G.A. § 21-2-300, authorizing the Secretary of State's mandatory statewide implementation of the BMD system. O.C.G.A. § 21-2-379.25(c) in essence, defines the preelection standard operational verification process required to implement the BMD election system specified in O.C.G.A. § 21-2-300.

Dr. Coomer, Dominion's Director of Product Strategy and Security, "absolutely" agreed in his hearing testimony "that one of the goals of logic and accuracy testing and equipment is to do some measure of confirmation that that the equipment is working properly." (Tr. Vol. II at 83.) His affidavit submitted earlier by Defendants both in 2019 and 2020 summarized in more detail the purpose and function of pre-election L & A testing in connection with the Dominion voting systems used in Georgia:

Dominion's optical scanners (ICP) can be used with BMD-marked paper ballots or hand-marked paper ballots. The ICP units do not interpret the human-readable (text) portion of either type of ballot. Instead, the ICP units are programmed to read the QR Code for the BMD ballot or particular coordinates on hand-marked ballot .... The target locations are then correlated to individual choices represented on the ballot. Pre-Logic and Accuracy Testing (Pre-LAT) is performed each election on every machine to verify that the target locations on hand-marked ballots, and the barcodes on BMD-marked ballots correspond correctly to the choices represented on the ballots and the digital cast-vote-records.

(Doc. 821-1 at 6.)

The Georgia State Election Board in early 2020 adopted a new Logic and Accuracy Testing Rule, SEB Rule 183-1-12.08.[54] This Rule requires:

1294*1294 During the public preparation and testing of the electronic poll books, electronic ballot markers, printers, and ballot scanners to be used in a particular primary or election, the election superintendent shall cause each electronic ballot marker and scanner to be programmed with the election files for the precinct at which the electronic ballot marker and ballot scanner unit will be used. The superintendent shall cause the accuracy of the components to be tested by causing the following tasks to be performed:
A. Check that the electronic poll books accurately look up and check-in voters via both the scanning function and manual lookup and create a voter access card that pulls up the correct ballot on the electronic ballot marker for every applicable ballot style.
B. Check that the touchscreen on the electronic ballot marker accurately displays the correct selections and that the touchscreen accurately reflects the selected choices.
C. Check that the printer prints a paper ballot that accurately reflects the choices selected on the touchscreen and immediately mark all printed paper ballots as "test" ballots.
D. Check that the ballot scanner scans the paper ballot, including both ballots marked by electronic ballot markers and ballots marked with a pen, and that the ballot scanner scans ballots regardless of the orientation the ballot is entered into the scanner.
E. Check that the tabulation contained in the ballot scanner memory card can be accurately uploaded to the election management system, and that the tabulated results match the selections indicated on the paper ballot.

Ga. Comp. R. & Regs, 183-1-12-.08(3)(A)-(E).

Yet the Secretary of State's January 20, 2020 published procedures for conducting L & A testing give an instruction for a fraction of the testing required under O.C.G.A. § 21-2-379.25(c) and its implementing regulation. (Doc. 809-4 at 25; Doc. 809-5 at 2-8.) The procedure's provision for "Testing the BMD and Printer" requires testing of only one candidate race per BMD for each ballot style (i.e., one designated vote for the presidential race and no other races or one designated vote for another office and nothing else). It also provides that "[a]ll unique ballot styles do not have to be tested on each BMD." (*Id.*) The published procedure gives this example for how to conduct the BMD machines' ballot testing: "Example: Ballot from BMD 1 contains a vote for only the first candidate in each race listed in Ballot style 1. Ballot from BMD 2 contains a vote only for the second candidate in each race on Ballot 1, and continue through the line of devices until all the candidates in all races within the unique ballot style will have received a single vote." (Doc. 809-4 at 25.) In other words, the testing instructions do not provide for a review of whether each BMD machine in the precinct can correctly produce candidate selections on the touchscreens, and aligned ballot results in turn on scanners and printers for all elective offices on the ballot. But whether a BMD machine or scanner may be able to accurately relay a vote designation for one office does not mean that it properly does so for all other races and offices listed on the ballot.

At the October 1, 2020 follow-up hearing to address the State's implementation of the brand new software modification on the BMDs, the Court explored whether the software change would impact the 1295*1295 scope of L & A testing procedures. The Court heard from Michael Barnes, Director of the Secretary's Center for Election Systems, who conducted acceptance testing on the BMD system prior to distribution of the software update to the 159 counties on or about September 29, 2020. The Court learned that Mr. Barnes was involved in the development of the logic and accuracy testing procedures, though Mr. Harvey, as Director of Elections, rather than Mr. Barnes apparently directly oversees their implementation. Mr. Barnes indicated that the counties were instructed to follow the original L & A protocols after verifying the new hash signature for the new version of the ICX software application. (October 1, 2020 Tr. at 35.) Mr. Barnes described a procedure for L & A testing that does not mirror the written instructions in the Secretary of State's January 2020 Procedures manual. Mr. Barnes has not been in the field to observe how counties are conducting the L & A testing pursuant to the instructions provided by the Secretary of State's Office. (*Id.* at 43.) Therefore, it is not clear what practices the counties are using in conducting their L & A testing, and it is entirely possible different counties employ different testing protocols or that they are implementing the narrow process delineated by Mr. Harvey and the January 2020 procedures guide. Even though the process as Mr. Barnes understands it is more expansive than the written guidance provided to the counties by the Secretary of State's Office, it is still incomplete when compared to the requirements of the statutory or regulatory provisions in terms of providing a full scope of testing of all ballot contests on every piece of the voting equipment.

Putting aside the intent and specifications of the L & A statutory provision, the Court looks at the basic purpose and function of L & A testing as a preliminary threshold standard for testing and ensuring the functionality of every voting machine to be used in an election by voters and capacity to produce pre-election an accurate record and tabulation of votes for candidates

appearing on the ballot. First, the Court has considered Dr. Coomer's explanation above that describes the baseline functional examination that L & A provides of voting balloting equipment — and how this translates into correct operation of voting machines, production of ballot results that correlate with ballot position, and vote tabulation. Next, it considers the testimony of Plaintiffs' expert, Mr. Kevin Skoglund, on this subject that goes into greater detail, along the same lines.

Mr. Skoglund, a cybersecurity expert with significant consulting experience with public jurisdictions, testified regarding the Secretary of State's L & A testing directive issued in January 2020. He explained that L & A testing is aimed at "verifying that every piece of equipment is going to operate properly and record votes properly on election day. And so we're crafting a set of questions to ask in advance to try and ascertain if that is true.... you would want to test every ballot style because you want every ballot style to work properly. And you want to check every contest. At a minimum, you want to make sure that every candidate is able to receive a vote .... But you also have to make sure that the votes aren't being swapped, that they are not crisscrossing." (Tr. Vol. III at 128.) Mr. Skoglund further clarified that this involves checking to make sure that "whatever you do on the screen is reflected in what is output in the end. On a tabulator, you're validating that when you take the input of the ballot into the tabulator that the totals that come out at the end match correctly. In both cases, you are looking to see if what goes in gives you what you expect to come out the other side." (*Id.* at 131-132.) Finally, he explained 1296*1296 how as an election consultant as well as when he has served as a poll manager/voting adjudicator in his home state of Pennsylvania, he has seen some dramatic systematic vote tallying failures that could have been prevented if the L & A testing had properly been handled and identified the issue causing these results that had to be reversed.[55] The tabulation for some races on a ballot also could be totally correct while for others, they were wrong and there were candidates who received zero votes. (*Id.* at 132-133.) In summary, "[i]f you are only auditing one race, you are only going to detect problems in one race. Once you test, the scope of your testing determines whether you will find the problems. If you don't look, you can't find problems." (*Id.* at 130.)

The Secretary of State's Director of Elections, Mr. Chris Harvey, provides an affidavit in this case that addresses the Secretary of State's L & A testing policy. He states the Secretary of State's Office designed the current L & A testing process "in consultation with Dominion and local election officials, and considered the best practices in doing so." (Doc. 834-3 ¶ 7.) In his opinion, the Coalition Plaintiffs' proposal that all races within the unique ballot style be tested is "overly burdensome and require[s] a test deck that is extremely large for each BMD." (*Id.* ¶ 6.) According to Mr. Harvey, the State/Dominion/local election officials group therefore concluded that the "increase in burden on local elections officials" would be "dramatic" and "unnecessary" if it conducted any more extensive L & A testing of the ballot than what is required in the January 2020 election procedures manual. *However, Dr. Coomer testified at the injunction hearing that he was not aware that the Georgia Secretary of State now is only requiring testing of one vote position on each ballot.* (Tr. Vol. II at 84.)

The Court understands Mr. Harvey's concern as to the testing burden. But the current state procedure slices and dices standard L & A protocols and objectives in testing for each voting machine (and scanner and printer) to only a small fraction of the electoral races for offices on the

ballots to be run on each machine in each County precinct. This is a serious short cut that truncates L & A testing's basic objective of checking on a pre-election basis the voting equipment and software's functionality as well as logic and accuracy in producing a useable, proper ballot printout and vote count, as discussed both by Mr. Skoglund and Dr. Coomer, and anticipated under Georgia law. This makes no sense when the goal is for the system to run smoothly on election day and produce ballots that accurately reflect citizens' votes cast on the BMD system tabulators.

The Court respects that the Secretary of State and Georgia State Election Board are vested with considerable discretion in implementing the mandate of O.C.G.A. § 21-2-379.25(c). However, the Secretary of State's January 2020 Procedures Manual is plainly inconsistent with the state statutory objective and requirements. The issue before the Court, though, is not whether any particular set of procedures is in full compliance with state law or a mere error in judgment by the Secretary of State's Office. Voters do not have a First or Fourteenth Amendment constitutional right to perfect implementation of state statutory provisions guiding election preparations and operations. But they do have the right to cast a ballot vote that is properly counted on machinery that is not compromised or that produces unreliable results. L & A testing is not complex. It is tedious — but it is essential homework that protects the 1297*1297 system and voters as the elections commence.

Recognizing that early voting starts on October 12, 2020 and the imminence of the November 3, 2020 general election, the Court must defer to the Secretary of State's Office and State Board of Elections determination of whether additional measures are pragmatically feasible at this juncture to strengthen the scope of L & A preparations for a general election with a huge anticipated turnout. As L & A testing has already commenced on BMD equipment to be deployed at early voting locations, the Court is not prepared to issue a ruling on the L & A testing issue purely standing on its own. Accordingly, the Court recommends that the Secretary of State and State Election Board expeditiously review in conjunction with Dominion: (1) the adequacy of the current January 2020 procedures, particularly in light of evidence of prevailing protocols used in states nationwide for conducting for logic and accuracy tests; (2) what modifications can and will be made by the time of the January 2021 elections runoffs and thereafter, or beforehand (if at all feasible). The Court further recommends that the process for evaluation and change in procedures shall be made public on a timely basis and that the results of such evaluation and any changes be made public on a timely basis.[56]

5. Audits

Plaintiffs assert that the Dominion BMDs should not be used in Georgia's elections because unlike hand-marked paper ballots the BMDs are unauditable. In conjunction with their request to enjoin the use of BMDs and to require handmarked paper ballots as the primary voting method for in-person voting, Plaintiffs request that the State be required to adopt more robust election audit procedures based on generally accepted audit principles. Specifically, the Coalition Plaintiffs' motion seeks an order "commanding the State Defendants to issue rules requiring meaningful pre-certification audits of election results, focusing on contested candidate races and ballot questions, with such auditing to be based on application of well-accepted audit principles in order to establish to a scientifically appropriate level of confidence that any incorrect

outcomes will be detected in time to be remedied prior to certification of results." (Doc. 809.) The Curling Plaintiffs similarly request that the Court order Defendants to file "a plan providing specific steps the Defendants intend to take to ... institute pre-certification, post-election, manual tabulation audits of the paper ballots to verify election results, in sufficient detail for the Court to evaluate its adequacy." (Doc. 785.)

Plaintiffs presented expert testimony from Dr. Philip Stark, a preeminent renowned statistician and original inventor and author of the risk-limiting audit ("RLA") statistical methodology for auditing election outcomes embraced by the 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").[57] (*See* Declarations of Dr. Philip A. 1298*1298 Stark, Docs. 296; 640-1 at 40-45; 680-1 at 2-24; 809-2; 853-1.) A risk-limiting audit is a "particular approach to catching and correcting incorrect election outcomes before they become official." (Stark Decl., Doc. 296 ¶ 27.)

As Dr. Stark explains, a RLA "offers the following statistical guarantee: if a full manual tally of the complete voter verifiable paper trail would show a different electoral outcome, there is a known, predetermined minimum chance that the procedure will lead to a full manual tally." (*Id.*) If the RLA "does lead to a full manual tally, the result of that manual tally replaces the reported outcome, thereby correcting it." (*Id.* ¶ 28.) In a RLA, "the `outcome' means the political result: the candidate(s) or position that won, or the determination that a run-off is needed, not the exact vote totals." (*Id.* ¶ 29.) "The maximum chance that the procedure will not lead to a full manual tally if that tally would show a different outcome is called the *risk limit.*" (*Id.* ¶ 30.) In other words, "the risk limit is the largest chance that the audit will fail to correct an outcome that is incorrect, where `incorrect' means that a full manual tally of the voter-verifiable paper trail would find different winner(s)." (*Id.*) For example, a RLA with "a risk limit of 5% has at least a 95% chance of requiring a full manual tally, if that tally would show an outcome that differs from the reported outcome." (*Id.* ¶ 31.)

According to Dr. Stark the "simplest risk-limiting audit is an accurate full hand tally of a reliable audit trail: Such a count reveals the correct outcome." Lindeman, M. and Stark, P., *A Gentle Introduction to Risk-Limiting Audits*, IEEE SECURITY AND PRIVACY, SPECIAL ISSUE ON ELECTRONIC VOTING (2012) at 1. Because a full hand count is administratively burdensome and time consuming, Dr. Stark designed the RLA as a method of examining far fewer ballots that "can provide strong evidence that the outcome is correct," where the "ballots are chosen at random by suitable means." *Id.* RLAs provide "statistical efficiency" because a RLA of an election "with tens of millions of ballots may require examining by hand as few as several hundred randomly selected paper ballots. A RLA might determine that more ballots need to be examined, or even that a full hand recount should be performed, if the contest is close or the reported outcome incorrect." NAS Report at 95.

1299*1299 The RLA methods Dr. Stark designed "conduct an `intelligent' incremental recount that stops when the audit provides sufficiently strong evidence that a full hand count would confirm the original (voting system) outcome. As long as the audit does not yield sufficiently strong evidence, more ballots are manually inspected, potentially progressing to a full hand tally of all the ballots."[58] *Id.* Whether the evidence is "sufficiently strong" is "quantified by the risk

limit, the largest chance that the audit will stop short of a full hand tally when the original outcome is in fact wrong, no matter why it is wrong, including `random' errors, voter errors, configuration errors, bugs, equipment failures, or deliberate fraud."[59] *Id.*

Risk-limiting audits "do not guarantee that the electoral outcome is right, but they have a large chance of correcting the outcome if it is wrong" but they do "guarantee that if the vote tabulation system found the wrong winner, there is a large chance of a full hand count to correct the results." Lindeman and Stark (2012) at 6. In order to provide this guarantee, a RLA must be based on a reliable and trustworthy audit trail produced by a voting system that is software independent. *Id.* at 1. (*See also* Stark Suppl. Decl., Doc. 680-1 ¶ 4; Stark Suppl. Decl. 640-1 at 42 ¶ 10.)

RLAs involve manually examining and interpreting randomly selected portions of an audit trail of ballots that voters had the opportunity to verify recorded their selections accurately. Lindeman and Stark (2012) at 1. The consensus among voting system experts is that the best audit trail is voter-marked paper ballots; voter-verifiable paper records printed by voting machines are not as good. *Id.*; *see also* NAS Report at 94-95.[60]

1300*1300 A voting system is strongly software independent "if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome, and moreover, a detected change or error in an election outcome (due to change or error in the software) can be corrected without re-running the election." (Stark Suppl. Decl., Doc. 640-1 at 42 ¶ 10.) "Systems based on optically scanning hand-marked paper ballots (with reliable chain of custody of the ballots) are strongly software independent, because inspecting the hand-marked ballots allows an auditor to determine whether malfunctions altered the outcome, and a full manual tabulation from the paper ballots can determine who really won, without having to re-run the election." (*Id.*) Therefore, a risk-limiting audit of an election conducted using hand-marked paper ballots "can guarantee a large chance of correcting the outcome if the outcome is wrong." (*Id.*)

Dr. Stark's affidavits and hearing testimony address the impossibility of conducting a reliable audit of ballots and voting totals derived from QR codes for purposes of verifying the accuracy or integrity of election results or processes. In Dr. Stark's view, the risk-limiting audit methodology cannot be properly utilized to assess the accuracy of election results in the context of a BMD system where ballots are tabulated based on a humanly non-readable QR code that is not voter verifiable and where the computer voting system is vulnerable to data hacking or manipulation that can alter votes cast in untraceable ways — including in the votes actually shown on the ballots that are audited.

In his December 15, 2019 declaration, Dr. Stark explains,

The most compelling reason for postelection audits is to provide public evidence that the reported outcomes are correct, so that the electorate and the losers' supporters have reason to trust the results. Audits that cannot provide evidence that outcomes are correct are little comfort. A transparent, full hand count of a demonstrably trustworthy paper record of votes can provide such evidence. So can a risk-limiting audit of a demonstrably trustworthy paper record of votes.

(Stark Suppl. Decl., Doc. 680-1 ¶ 3.) But if "there is no trustworthy paper trail, a true risk-limiting audit is not possible, because an accurate full manual recount would not necessarily reveal who won." (*Id.* ¶ 4.) Unlike voting systems using optical scan hand-marked paper ballots, BMD based voting systems are not strongly software independent. (Stark Suppl. Decl., Doc. 640-1 at 42 ¶ 10.) According to Dr. Stark, a BMD "by its nature, erases all direct evidence of voter intent." (Tr. Vol. I at 46.) There is no way to tell from a BMD printout what the voter actually saw on the screen, what the voter did with the device, or what the voter heard through the audio interface. (*Id.*) For this reason, there is no way to establish that a BMD printout is a trustworthy record of what the BMD displayed to the voter or what the voter expressed to the BMD. (Stark Suppl. Decl., Doc. 680-1 ¶ 10.) Because a BMD printout cannot be trusted to reflect voters' selections, auditors can only determine whether the BMD printout was tabulated accurately, not whether the election outcome is correct. (Stark Suppl. Decl., Doc. 640-1 at 42 ¶ 10.) Nor can auditors determine the correct outcome under these circumstances. (*Id.*) Therefore, because a BMD printout is not trustworthy, "applying risk-limiting audit procedures to [a] 1301*1301 BMD printout does not yield a true risk-limiting audit." (*Id.* ¶ 4.)

Plaintiffs provided additional affidavits, testimony, and evidence from other nationally recognized experts that addressed their similar views that the QR code based voting system does not produce a reliable voter-verifiable audit trail that can be audited consistent with established RLA standards and foundation principles. (*See* Decls. of Dr. Andrew W. Appel, Doc. 681-3, Doc. 855-3; Decls. of Dr. Alex Halderman, Doc. 619-2, Doc. 682, Doc. 692-3; Decls. Of Dr. Richard A. DeMillo, Doc. 680-1 at 45-56, Doc. 716-1; *see also* Doc. 615-2, Wenke Lee, Ph.D., Secure, Accessible & Fair Elections Commission, *Basic Security Requirements for Voting Systems* (October 8, 2018); Andrew A. Appel, Richard A. DeMillo, Philip B. Stark, *Ballot-marking devices (BMDs) cannot assure the will of the voters* (April 21, 2019); Doc. 692-3 at 8-23, Bernhard, M., A. McDonald, H. Meng, J. Hwa, N. Bajaj, K. Chang, and J.A. Halderman Can Voters Detect Malicious Manipulation of Ballot Marking Devices? IEEE Proc. Security & Privacy, 1, 679-694 (2020)).

Dr. Halderman has explained the many ways a BMD could be maliciously programmed or otherwise malfunction such that the ballot printed by the BMD does not match the voter's intended selections. He also attests that "if voters do not reliably detect when their paper ballots are wrong, no amount of post-election auditing can detect or correct the problem." (Halderman Decl., Doc. 619-2 ¶ 12.) Dr. Halderman, along with others at the University of Michigan, conducted experiments to determine how often voters fail to notice that their BMD printed ballots differ from the selections made on the touchscreen voting machines. (*Id.* ¶ 13.) When not given any prompting to review their ballots, only 6.5% of participants in the study noticed their votes had been changed by the BMD. (*Id.* ¶ 14.)

Between November 2018 and March 2019, Dr. Appel conducted a research collaboration with Dr. DeMillo of Georgia Tech and Dr. Stark, leading to the publication of a joint paper, Ballot Marking Devices (BMDs) Cannot Assure the Will of the Voters. After analyzing the consequences of a study of whether voters review ballot cards produced by BMDs, their research concluded:

Risk-limiting audits of a trustworthy paper trail can check whether errors in tabulating the votes as recorded altered election outcomes, but there is no way to check whether errors in how BMDs record expressed votes altered election outcomes. The outcomes of elections conducted on current BMDs therefore cannot be confirmed by audits.

(Appel Decl., Doc. 681-3 ¶¶ 11, 13, 21.)

Dr. Wenke Lee, the only cybersecurity expert appointed to the Georgia Secretary of State's "Secure, Accessible & Fair Elections Commission," echoed Dr. Stark's opinions in advising the Commission on basic security requirements for voting systems:

In order to support risk-limited — auditing, paper ballots must be easily and clearly readable and manually countable. In particular, a paper ballot must show each and every vote exactly as cast by the voter. It cannot be just a summary of the votes (e.g., only a tally, or only the presidential ballot and not the down ballots). A manual count absolutely cannot rely upon a barcode, QR code, or any other kind of encoding scheme that is readable only by a machine because the cyber system that reads those codes also can be compromised and lie to the voter or auditor. In short, during a manual review, a human must be able to 1302*1302 clearly see evidence of the voter's original act.

(Doc. 615-2 at 3.)

In the face of this consensus as to the role of voter verification and auditing in ensuring voters' ballots are properly and accurately counted, and that the voting tallies are reliable, the State Defendants presented two rebuttal expert witnesses regarding the viability of conducting a valid risk-limiting audit of a QR code based voting system. Both Dr. Gilbert and Dr. Adida's declarations focused on the RLA as the essential tool for protecting against voting system mishaps in the implementation of a BMD system. (Doc. 834-2 at 7; Doc. 658-3 at 13-14, 20-21.)

Professor Juan Gilbert, Professor and Chair of the Computer & Information Science & Engineering Department of the University of Florida and leader of the Department's Human Experience Research Lab[61] testified regarding his views as to the value and reliability of RLA as part of the BMD system, which he endorses. Dr. Gilbert's research currently focuses on human use of technology and access to voting systems as opposed to issues involving cybersecurity issues or statistical methodology. He described the access benefits of the BMD system and addressed why in his view, voters will verify their printed ballots and therefore enable a meaningful RLA audit which he saw as a vital protective device. Dr. Gilbert has himself not performed any studies of voter review of ballots at the polls. The Court notes that Dr. Halderman has recently published an article on this very subject.[62] Dr. Gilbert's risk/benefit assessment of the vote integrity or manipulation risks entailed in a QR code BMD system clearly differed from Plaintiffs' experts — and specifically Dr. Appel, Dr. Halderman, and Dr. Stark's views regarding the risks posed by the BMD system's reliance on tabulating votes based on a humanly unverifiable QR code.

Dr. Benjamin Adida is co-founder and Executive Director of VotingWorks, a non-profit vendor of election auditing technology and more recently, voting systems in the United States, including

accessible ballot-marking devices and hand-marked ballots.[63] Dr. Adida holds a PhD in cryptography and information security from MIT and has significant experience in the private and public sector. While his academic background is impressive, Dr. Adida's background and expertise is not specifically in statistics.[64]

1303*1303 VotingWorks contracts with multiple jurisdictions, assisting in the design and implementation of RLAs. According to Dr. Adida, "[t]he deployment of RLAs is challenging" and highly variable between jurisdictions. To date Georgia has contracted with VotingWorks for guidance in the development and implementation of a RLA in Georgia of one major statewide race every two years to be selected by the Secretary of State, under new rules adopted by the State Board of Elections. Ga. Comp. R. & Regs. 183-1-15-.04. Georgia is the only state so far that Voting-Works has contracted with that uses BMDs for all in-person voting.[65] (Tr. Vol. II at 285.)

Dr. Adida's methodology contained the inherent assumption of voter ballot verification. Dr. Adida testified that "[i]f the paper ballots have a chance to be verified by the voter, they can be used in a RLA whether they were BMD-produced or hand-marked produced." (*Id.* at 284.) Under the State's audit procedures, the RLA is conducted on the human readable text of the BMD ballot printout, not on the QR code. (*Id.* at 294; Adida Decl., Doc. 934-2 ¶ 12.) Therefore, according to Dr. Adida, "[a]s long as voters verify the text, and as long as RLAs are conducted on the basis of the same ballot text, then potential QR code mismatches are caught just like any other tabulation mistake might be caught. A successful RLA thus provides strong evidence that, if there were QR code mismatches, they did not affect the outcome of the election." (Adida Decl., Doc. 934-2 ¶ 12.)

Dr. Stark has submitted two affidavits in which he severely criticizes the premise of Dr. Adida's position that a valid RLA or valid RLA results can be conducted in the context of a BMD election in which there is no meaningful audit trail and voters cannot verify the QR code, among other things.[66]

First, despite Dr. Adida's assumption that BMD voters will review and verify their ballot selections on the ballot printout, the overwhelming evidence from actual studies of voter behavior "suggests that less than ten percent of voters check their printouts and that voters who do check often overlook errors." (Stark Suppl. Decl., Doc. 680-1 ¶¶ 14, 30(d); Stark Suppl. Decl., Doc. 891 ¶¶ 9-10, 12.) In an actual election, there is no way to know how many voters checked their BMD printouts for accuracy. (Stark Suppl. Decl., Doc. 891 ¶ 16.) "The fact that a voter has the opportunity to check the BMD printout does not make a BMD printout trustworthy." (*Id.* ¶ 7.)

1304*1304 Second, Dr. Stark categorically disagrees with Dr. Adida's position that a post-election RLA can demonstrate that BMDs function correctly during elections. According to Dr. Stark — whose opinions are affirmed by other experts — audits of BMD-marked ballot printouts cannot reliably detect whether malfunctioning BMDs printed the wrong votes or omitted votes or printed extra votes (whether due to bugs, configuration errors, or hacking).[67] And "this is true even if the malfunctions were severe enough to make losing candidates appear to win." (*Id.* ¶ 5.) Dr. Stark testified that "[t]here is no audit procedure that can be conducted on the output of

ballot-marking devices to confirm that the outcome of a contest is correct in the sense that it reflects what the voters actually did on the BMD or saw on the screen or heard through the audio." (Tr. Vol. I at 68.) "[U]nless virtually every voter diligently checks the printout before casting it, there is no reason to believe that an accurate tabulation of BMD printouts will show who really won." (Stark Suppl. Decl., Doc. 680-1 ¶ 13.)

The fundamental disagreement between Dr. Stark and Dr. Adida boils down to the purpose and function of a risk-limiting audit. Dr. Adida testified at the hearing that the "point of a RLA is to check the tabulation of the votes matches what the voters saw on the paper ballot" and that the "most important function" of a RLA "is to make sure that bugs, malfunctions, dust on the scanner, [or] nation state attacks do not corrupt that function." (Tr. Vol. II at 292.) According to Dr. Stark, ballot polling risk-limiting audits, the audit method piloted and planned in Georgia, do not check the tabulation of votes, per se.[68] (Stark 1305*1305 Suppl. Decl., Doc. 809-2 ¶ 12.) They do not check whether the votes were recorded or tabulated correctly. (*Id.* ¶¶ 12, 13(b).) Ballot-polling risk limiting audits do not check the tabulation of any individual BMD ballot or any group of ballots, except in the sense that they check whether the reported total was wrong by more than the reported margin. (*Id.* ¶ 13(c).) Ballot-polling audits only check whether a full hand count of the BMD printout would find the same winners by checking whether the paper trail has more votes for the reported winner than for any other candidate. "The tabulators could misread every single vote and still find the correct winner" and a ballot-polling audit would not detect this because the outcome could be "correct despite the complete mistabulation." (*Id.* ¶ 12; Stark Suppl. Decl., Doc. 680-1 ¶¶ 20-21.) For this reason, "it is incorrect to consider ballot-polling RLAs to be checks of the tabulation system." (Stark Suppl. Decl., Doc. 891 ¶ 15; Stark Suppl. Decl., Doc. 680-1 ¶¶ 20-21.)

A ballot-polling audit of a contest conducted on a BMD system cannot confirm the reported outcomes are correct because it cannot show that the BMDs functioned correctly. (Stark Suppl. Decl., Doc. 680-1 ¶ 21.) All such an audit can do is provide statistical evidence that a full manual tabulation of the BMD printouts would find the same winner that was reported in the audited contest.[69] (*Id.*) "If the BMD printouts contained outcome-changing errors, the audit would have no chance of detecting that, nor of correcting the reported outcomes." (*Id.*)

This is essentially what the pilot audits Georgia has conducted accomplish and what the planned audit for the selected contest in the November 2020 election will accomplish.[70] However, this does not serve 1306*1306 the purpose and function of a true risk-limiting audit as designed by Dr. Stark to statistically guarantee that the audit will produce a large chance of correcting the election outcome if the reported outcome is wrong.[71]

Additionally, the Court pursued a range of questions with Dr. Adida when he testified about VotingWorks' application of the RLA for the first time in a state of Georgia's size in solely one race under these circumstances. The Court cannot say that it got close to understanding the rationale or specific contours of the sampling methodology to be used by Voting Works.

Suffice it to say, the experts here are in hot debate and approach these issues from different backgrounds and areas of expertise. The Court recognizes that the RLA is deemed by all of the experts as a control valve essential to election integrity. The question they differ on is whether a

RLA can be validly implemented in the context of Georgia's QR code BMD voting system. While the Plaintiffs have marshalled a formidable amount of evidence that casts serious doubt on the validity of the use of the RLA with the current system (including the specific RLA methodology that Voting-Works is pursuing here), unless the Court determines that the BMDs must be enjoined from use in Georgia's upcoming elections, the requested remedy appears irrelevant. Absent such an injunction, there is no audit remedy that can confirm the reliability and accuracy of the BMD system, as Dr. Stark has stressed. Plaintiffs do not request, and have not offered, any other proposed audit procedures to accomplish the goal of the RLA. Nor is the Court in a position to reach a judgment regarding whether the Secretary of State's plan to conduct a single RLA assessment in one statewide race under these circumstances provides any meaningful protection or guidance regarding the accuracy of tabulation of the overall voting results (or system). The Court has some major doubts, given the entirety of the evidence discussed here. But under O.C.G.A. § 21-2-498(e) the Secretary of State will be required to implement risk-limiting auditing for all statewide elections "beginning not later than November 1, 2024." The Secretary and State Election Board still have the opportunity to consider other options for effectuating a somewhat more meaningful RLA process — i.e., by at very least strengthening voting protocols for the 2022 election cycle to encourage voters' ballot verification and expanding the number of electoral contests audited. That said, the 1307*1307 specific relief Plaintiffs ask for ultimately rises or falls on whether the evidence as a whole establishes the Plaintiffs' likelihood of success on their challenge of the current QR barcode-based BMD system. And the auditing issues considered are relevant to this central claim.

6. Analysis of Preliminary Injunction Standards as Applied to Plaintiffs' Primary BMD Vote Related Claims

The Court has in Section II A. above discussed the standards the Court must weigh and apply in determining the Plaintiffs' entitlement to preliminary injunctive relief. The Court must first consider whether Plaintiffs have established a substantial likelihood of prevailing on the merits of their claims and related to that, "consider the character and magnitude of the asserted injury to the rights protected by the First and Fourteenth Amendment." *Anderson*, 460 U.S. at 789, 103 S.Ct. 1564.

The interest Plaintiffs seek to vindicate now is the same interest at stake when they brought this litigation under the old voting system in 2017. As the Court first recognized in its August 2018 Order, the Constitution affords Plaintiffs an interest in transparent, fair, accurate, and verifiable election processes that guarantee each citizen's fundamental right to cast an accountable vote. Plaintiffs assert they will suffer immediate and irreparable harm to this interest if required by the State to cast a ballot on the BMD system that cannot be confirmed or verified as reflecting their actual vote choices because the votes are tabulated solely from a computer generated QR barcode that is not human-readable and is vulnerable in the current system to failure or breach. They further assert that this injury is exacerbated because votes cast by BMDs pose the significant risk of having the votes altered, diluted, or effectively not counted.[72] Plaintiffs have shown demonstrable evidence that the manner in which Defendants' alleged mode of implementation of the BMD voting system, logic and accuracy testing procedures, and audit protocols 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).

The Court views the burden and the threatened deprivation as significant under the *Anderson/Burdick* balancing framework. The right to vote derives from the right of individuals to associate for the advancement of political beliefs that is at the core of the First Amendment and is protected from state infringement by the Fourteenth Amendment. *E.g.*, *Williams v. Rhodes*, 393 U.S. 23, 30-31, 89 S.Ct. 5, 21 L.Ed.2d 24 (1968); *NAACP v. Button*, 371 U.S. 415, 430, 83 S.Ct. 328, 9 L.Ed.2d 405 (1963). "Writing for a unanimous Court in *NAACP v. Alabama* [357 U.S. 449, 78 S.Ct. 1163, 2 L.Ed.2d 1488 (1958)], Justice Harlan stated that it `is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the `liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech.'" *Anderson*, 460 U.S. at 786-87, 103 S.Ct. 1564 (internal citation omitted). As discussed in both the Court's September 28, 2020 Order and this Order, the individual Plaintiffs have a strong preference to cast votes in person and do not want to be 1308*1308 shunted out of the regular exercise of the shared political experience of voting with their fellow citizens at their local precinct location. The First and Fourteenth Amendments afford them this right to associate for the advancement of political beliefs by exercising the franchise at the voting booth and to cast their votes effectively. *See generally*, *Anderson*, 460 U.S. at 788, 103 S.Ct. 1564; *Williams v. Rhodes*, 393 U.S. 23, 30-31, 89 S.Ct. 5, 21 L.Ed.2d 24 (1968); *Reynolds v. Sims*, 377 U.S. 533, 563, 84 S.Ct. 1362, 12 L.Ed.2d 506 (1964).

"Since the right to exercise the franchise in a free and unimpaired manner is preservative of other basic civil and political 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. "It does not follow, however, that the right to vote in any manner and the right to associate for political purposes through the ballot are absolute." *Burdick v. Takushi*, 504 U.S. 428, 433, 112 S.Ct. 2059, 119 L.Ed.2d 245 (1992). "Although these rights of voters are fundamental, not all restrictions imposed by the States ... impose constitutionally-suspect burdens on voters' rights to associate or to choose among candidates." *Anderson*, 460 U.S. at 788, 103 S.Ct. 1564. Rather, the Supreme Court has recognized that States retain the power to regulate their elections to provide fairness, honesty, and order in the democratic process. *Id.* The right to vote is the right to participate in an electoral process that is necessarily structured to maintain the integrity of the democratic system. *Anderson*, 460 U.S. at 788, 103 S.Ct. 1564. "To achieve these necessary objectives, States have enacted comprehensive and sometimes complex election codes." *Id.* Election laws "invariably impose some burden upon individual voters," whether they govern the "registration and qualifications of voters, the selection and eligibility of candidates, or the voting process itself," and such laws "inevitably affect[] — at least to some degree — the individual's right to vote and his right to associate with others for political ends." *Id.*; *Burdick*, 504 U.S. at 433, 112 S.Ct. 2059. But, "cumbersome election machinery can effectively suffocate the right of association, the promotion of political ideas and programs of political action, and the right to vote." *Williams*, 393 U.S. at 39, 89 S.Ct. 5 (Douglas, concurring). And, "[w]hen 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*, 377 U.S. at 566, 84 S.Ct. 1362 (quoting *Gomillion v. Lightfoot*, 364 U.S. at 347, 81 S.Ct. 125).

Georgia's Election Code mandates the use of the BMD system as the uniform mode of voting for all in-person voters in federal and statewide elections. O.C.G.A. § 21-2-300(a)(2). The statutory provisions mandate voting on "electronic ballot markers" that: (1) use "electronic technology to independently and privately mark a paper ballot at the direction of an elector, interpret ballot selections, communicate such interpretation for elector verification, and print an elector verifiable paper ballot;" and (2) "produce paper ballots which are marked with the elector's choices in a format readable by the elector" O.C.G.A. § 21-2-2(7.1); O.C.G.A. § 21-2-300(a)(2).

Plaintiffs and other voters who wish to vote in-person are required to vote on a system that does none of those things. Rather, the evidence shows that the Dominion BMD system does not produce a voter-verifiable paper ballot or a paper ballot marked with the voter's choices in a format readable by the voter because the 1309*1309 votes are tabulated solely from the unreadable QR code. Thus, under Georgia's mandatory voting system for "voting at the polls"[73] voters must cast a BMD-generated ballot tabulated using a computer generated barcode that has the potential to contain information regarding their voter choices that does not match what they enter on the BMD (as reflected in the written text summary), or could cause a precinct scanner to improperly tabulate their votes.

As a result, each of the Plaintiffs attest that they are forced to forego their right to full and unfettered participation in the political process and to alternatively exercise their right to vote using Georgia's absentee ballot regime which carries its own burdensome procedures, though they may be minimal as compared to the burdens created by the BMDs.[74] Absentee voting itself has been the subject of much constitutional litigation where the implementation of these procedures resulted in the rejection of absentee ballots and voter disenfranchisement. To avoid being denied the ability to verify their votes on the BMD system, Plaintiffs must trade one unfavorable burden for another. Plaintiffs are left with the choice of having to run another gauntlet of the absentee voting process because of potential uncertain postal delivery issues, untimely processing by the registrar's office, signature matches, etc. As discussed in Section III D herein, Plaintiffs have shown a significant burden resulting from the accuracy and voter invalidation issues that affect Dominion's scanner/tabulators and adjudication software used for determining voter intent and tallying hand-marked absentee ballots. A choice between two evils is no choice at all; the Equal Protection Clause guarantees the opportunity for equal participation by all voters in the election regardless of which method they choose to cast their vote.

That Plaintiffs and other voters have the alternative of casting an absentee hand-marked paper ballot does not lessen or absolve the State of the burdens imposed 1310*1310 by the State's chosen, preferred, primary voting system, in which it invested hundreds of millions of taxpayer dollars. The State opposes a court-ordered switch to hand-marked paper ballots for in-person voters at the polls. The State does not wish to be forced into an administratively burdensome system of carrying out an election using hand-marked ballots and voters do not wish to be forced into an absentee regime that contains its own distinct array of burdens and uncertainties associated with whether the ballot will be accepted and counted.

While the Court recognizes Plaintiffs' strong voting interest and evidentiary presentation that indicate they may ultimately prevail in their claims, the Court must perforce address the posture of this case as a whole as well as the Plaintiffs' burdens "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); *New Georgia Project v. Raffensperger*, 976 F.3d. 1278, 1280-81 (11th Cir. 2020).

In election cases, the Supreme Court and Eleventh Circuit have made ever more abundantly clear the mandate that district courts must exercise great restraint in considering the grant of injunctive relief that requires new rules on the cusp of an election where the Court's Order could cause electoral disruption and voter confusion. *Purcell v. Gonzalez*, 549 U.S. 1, 4-5, 127 S.Ct. 5, 166 L.Ed.2d 1 (2006); *Republican National Committee v. Democratic National Committee*, ___ U.S. ___, 140 S.Ct. 1205, 1207, 206 L.Ed.2d 452 (2020); *Republican Nat'l Comm. v. Common Cause R.I.*, ___ U.S. ___, 141 S.Ct. 206, 206, 207 L.Ed.2d 1154 (2020); *Merrill v. People first of Alabama*, ___ U.S. ___, 141 S.Ct. 190, 207 L.Ed.2d 1113 (2020); *New Georgia Project v. Raffensperger*, 976 F.3d at 1282. The Court expressed its concerns anew to Plaintiffs' counsel about this timing issue when Plaintiffs filed a renewed motion for preliminary injunction in August 2020, shortly after the denial without prejudice of their initial October, 2020 preliminary injunction motions targeting the BMD system and other voting practices.[75] The timing of the relief sought plays a paramount role in the evaluation of the practicality of granting the requested remedy at this point.

Litigation since Plaintiffs' amendment of their claims to include a challenge to the BMD system as a whole has stretched on since October 2019, with plenty of delays occurring. But these delays were not attributable to any lack of litigation diligence or aggressiveness on Plaintiffs' counsel's part. For a variety of reasons, including multiple motions to dismiss that stalled discovery, the Court's own schedule especially after the advent of the Covid-19 pandemic, and challenges posed by the difficulty of the case as a whole, Plaintiffs' motions for preliminary injunction were not heard until September in this Presidential election cycle year. Some evidentiary 1311*1311 challenges at that point reared their heads. Due to Dominion's own historic unwillingness to provide independent cybersecurity researchers with access to the Dominion Suite software and equipment package (through sale or otherwise), Plaintiffs obtained only last-minute, court-ordered access to the Dominion system for hands-on testing. Finally, as State Defendants have not maintained a practice of regular independent cybersecurity testing and evaluation of vulnerability issues in their own systems impacting the elections realm and had asserted work product privilege over the one extant report, these types of reports were not available to the parties or Court when the hearing was about to commence.

Plaintiffs have presented a massive and complex record in this matter for the Court's review that has consumed its attention for long swaths of time. Plaintiffs also in the course of their hearing preparation presented an expanded array of expert affidavits as well as voter and election evidence, collected primarily from the June and August 2020 statewide primary and runoff elections. These elections produced more substantive empirical evidence and helped to bring into sharper focus the evidentiary issues in this case.

Defendants also have presented substantive evidence in support of their overarching legal defense. They generally minimize the claims, concerns, and risk threats documented in Plaintiffs' challenge. At core, the State Defendants' counsel argue that Plaintiffs' legal claims boil down to

their disagreement with the policy choices legally vested in the Secretary of State and State Election Board's purview. In turn, they contend that Plaintiffs have suffered no cognizable threat of harm or burden in their exercise of their First and Fourteenth Amendment rights. Defendants also maintain that they have taken sufficient proactive measures in implementation of the new voting system to ensure its security and reliability.

The preliminary injunction hearing started on September 9, 2020 and concluded on September 13, 2020. But that was not the end, by any means, of the parties' continuing supplemental submissions to the Court. And record developments such as the State Defendants and Dominion's last-minute introduction of a modified system-wide software change to the voting system and dealings with the EAC continued to roll out before the Court — some of which was directly relevant to the evidentiary issues before the Court. Early voting in Georgia with the use of BMD voting machines, will commence now in one day, on October 12, 2020.

Some of Plaintiffs' claims pursued involved discrete and limited relief that do not upset the election apple cart. The Court has considered relief in two instances where there was strong evidence of state-imposed burdens to Plaintiffs' First Amendment constitutionally protected exercise of the franchise as well as narrowly tailored relief that was fully consistent with state law. The Court in those instances balanced the state's interests and burdens as well as relief issues relative to the operation of the elections before granting any form of narrowly tailored relief or delaying such relief until after the election. Indeed, the Court's Pollbook relief[76] was expressly framed based on the State's emergency ballot voting statutory and regulatory provisions to ensure that these emergency procedures could pragmatically be implemented on Election Day, November 3, 2020, if necessary so as to mitigate the severe burdens experienced by Plaintiffs and other voters in casting votes in 1312*1312 the new BMD-equipped system during the June and August 2020 elections.

By comparison, the Plaintiffs' BMD systemic injunctive challenge and request for replacement of the system with hand-marked paper ballots pose relief issues of an entirely different, more expansive scope. After reviewing all of the evidence in scrupulous detail, the Court must step back at this juncture, despite the persuasive evidence that Plaintiffs have provided. Plaintiffs' central claim seeks statewide relief, requesting that the Court enjoin implementation of the State's newly designated BMD voting system under O.C.G.A. § 21-2-300 and require instead the state's implementation of a hand-marked ballot system in its 159 counties. The problems posed obviously go beyond whatever the State's and counties' purported capacity issues are in connection with the purchase of ballot paper stock or printing arrangements. The requested relief would entail a fundamental modification in the election system that the Secretary of State and county election offices are not now equipped or prepared to administer. The Court has already seen in the record of this case enough election chaos, operational deficiencies, and challenges on all levels, plus stress in the system spiked further by Covid-19 complications, that the Court cannot embrace a rosy view of the simplicity of moving to a total, comprehensive paper ballot system with so little time to prepare for such a major transition. And this would likely have been true also even if such relief had been ordered on September 15th, the day after the injunction hearing concluded, based on election operations evidence presented in connection with the hearing. The substantial risks and long-run threats posed by Georgia's BMD system, at least as currently configured and implemented, are evident. However, the Court — especially after

reviewing evidence regarding election staff management and operations challenges in the June and August 2020 elections — cannot envision that state and county elections staff (including paid temporary contract personnel) would be equipped to move the system and voters through such a major operational change without chaotic disruptions occurring anew.

Risks are posed both by a sudden shift to a statewide hand-marked paper system and proceeding with the BMD system. Ultimately, the Court must find that imposition of such a sweeping change in the State's primary legally adopted method for conducting elections at this moment in the electoral cycle would fly in the face of binding appellate authority and the State's strong interest in ensuring an orderly and manageable administration of the current election, consistent with state law. So, for this reason alone, despite the strength of Plaintiffs' evidence, the Court must decline the Plaintiffs' Motions for Preliminary Injunction.

C. Coalition Plaintiffs' Claims Relating to Ballot Secrecy

The Coalition Plaintiffs seek to enjoin the use of BMDs on the basis that they severely burden the fundamental right to vote by depriving voters of secrecy of the ballot. They assert two theories as to how BMDs result in the deprivation of ballot secrecy: (1) the large size of the BMD touchscreens, if not configured to shield the screens from public view, permit anyone in the polling place to observe how a voter is voting; and (2) the precinct scanners record timestamp information such that a voted BMD ballot card can be traced back to the individual in-person voter by comparing the timestamps on the scanned cast vote records with the order in which voters used the machines.

1313*1313 In support of their first challenge, the Coalition Plaintiffs presented declaration testimony from 7 individuals who served as poll watchers in the June and August elections that the BMD touchscreens were clearly visible to the public from 30 to 50 feet away during the voting process. Additionally, there was some affidavit evidence of voter discomfort at the perception of the exposure of the voting process. (*See* Doc. 853-4 at 25.) Despite these observations, Plaintiffs have not established a resulting First Amendment injury where there is no evidence from any Plaintiff or any other voter claiming that the publication of their vote selections subjected them to threats, harassment, reprisals, or other "chilling" of the free exercise of the franchise from either Government officials or private parties. *See* *Buckley v. Valeo*, 424 U.S. 1, 64, 74, 96 S.Ct. 612, 46 L.Ed.2d 659 (1976) (per curiam); *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 343, 115 S.Ct. 1511, 131 L.Ed.2d 426 (1995) (noting that the "respected tradition of anonymity in the advocacy of political causes ... is perhaps best exemplified by the secret ballot, the hard-won right to vote one's conscience without fear of retaliation"); *Citizens United v. Federal Election Comm'n*, 558 U.S. 310, 366-67, 130 S.Ct. 876, 175 L.Ed.2d 753 (2010).

For Plaintiffs, this is an all or nothing proposition, as they seek to enjoin the BMDs outright and do not propose other solutions to the ballot secrecy problems posed by the oversize BMD touchscreens. However, it is not necessary to scrap the new voting machines where a less burdensome fix exists. Georgia's Election Code places the responsibility of arranging voting equipment at polling places to ensure voter privacy with "the governing authority of each county and municipality." O.C.G.A. § 21-2-267. The Secretary of State's Office has undertaken

measures to instruct local election officials on proper polling place layout and arrangement of BMDs to maintain voter privacy. (Harvey Decl. ¶ 3, Doc. 834-3; Ex. 1 to Harvey Decl., Doc. 834-3 at 7-11) ("The Secretary of State's office has provided guidance to county election officials about the setup of precincts so that [touch]screens will not be visible to other voters when they are being used by a voter."). If the counties fail to follow the requirements of O.C.G.A. § 21-2-267 and the guidance provided by the Secretary of State and voter privacy rights are violated, the State Election Board can undertake an investigation and/or enforcement action as necessary.

In support of their second contention, Plaintiffs assert that the "Dominion precinct scanners record timestamp information directly onto the digital cast vote record that is created when a ballot is scanned, with the result that a voted BMD ballot card can easily be connected afterward with the individual voter who cast that ballot by simply comparing the scanned cast vote records (ordered by timestamps) with the order in which voters are observed going through the voting process." (Br. Supp. Mot., Doc. 809-1 at 32-33.)

The Coalition Plaintiffs have not offered a single instance of actual infringement of voter anonymity as a result of the use of digitally recorded scanner timestamp records. And despite the lack of evidence of any local election official going to such great lengths to discover how someone voted, the evidence in the record describing and illustrating how the precinct scanners actually operate does not bear this out.

Instead, the Coalition Plaintiffs rely on scanned ballot images from Fulton County bearing timestamps recorded by the ICC central count scanner used to tabulate absentee and provisional ballots by election 1314*1314 personnel at the county election office. The timestamp recorded on the digital record of ballots tabulated by the ICC correlates to the time the ballot is run through the scanner by an election official and has no demonstrated correlation to the individual voter having marked an absentee ballot at home (or a voter having marked a provisional ballot at the precinct). *See* O.C.G.A. § 21-2-386 (providing that "[t]he process for opening the inner envelopes of and tabulating absentee ballots on the day of a primary, election, or runoff as provided in this subsection shall be a confidential process to maintain the secrecy of all ballots). The Coalition Plaintiffs have not offered any theory to suggest that absentee and provisional ballots can be linked back to individual voters using the timestamp recorded in the digital record by the ICC central scanner.

Unlike the ICC central scanner, the ICP precinct scanner does not record a digital timestamp on the ballots of in-person voters. Rather, ballots scanned on the ICP precinct scanner/tabulator includes a "randomized sequence number" that "preserves voter anonymity as there is no way to correlate the sequence number to either an individual voter, or a specific point in time that the ballot was cast. When results and images are stored on the removable memory (Compact Flash cards), no date-timestamp information is included which prevents the ability to recreate the sequence of how the ballots were cast thus preserving voter anonymity." (Coomer Decl. ¶ 10; Doc. 821-1; *see also* Ex. 19-A to Decl. of Marilyn Marks, Doc. 853-4 at 6 (showing ballot image from ICP scanner without any timestamp).) Dr. Coomer confirmed this again at the September 11 hearing, stating that there is no timestamp associated with ballot images scanned and stored in the digital cast vote records created by the ICP precinct scanner/tabulator. (Tr. Vol. II at 91-92.)

Accordingly, the Coalition Plaintiffs have failed to establish a likelihood of succeeding on the merits of their claim that the BMD system violates their right to ballot secrecy.

D. Hand-Ballot Scanning and Its Impact on Counting of the Vote

The Coalition Plaintiffs request that the Court require the State Defendants "to adopt scanning threshold settings for the Dominion scanners and vote review procedures that will ensure all voter marks on mailed and hand marked paper ballots are counted." (Br. Supp. Mot., 809-1 at 10.) They assert that the Dominion scanner and tabulation software and equipment are failing to count all legal votes as defined under Georgia law, resulting in an unconstitutional denial of review of the ballot before arbitrarily discarding perceptible ballot votes containing such marks. Plaintiffs contend that Defendants' challenged practices in connection with scanning and tabulation of such hand ballot votes violate Georgia law, which requires votes to be counted if the intent behind a voter's mark can be ascertained upon review. *See* O.C.G.A. §§ 21-2-438(b) & (c); *see also* O.C.G.A. § 21-2-483(g) (requiring manual review by the vote review panel of any overvote detected by the central tabulator).[77] And 1315*1315 Plaintiffs also argue the current system and its configuration is a violation of equal protection because in-person voters who use BMD voting machines are not subject to having their votes rejected by a scanner due to faint marks. Each of the individual Plaintiffs additionally have submitted affidavits in this case indicating that while they strongly prefer to vote in person, they have felt compelled to vote by absentee ballot because of their concerns about whether their ballots would be accurately counted in the State's BMD and prior DRE systems. (Decl. of Donna A. Curling, Doc. 785-3; Decl. of Donna Price, Doc. 785-4; Decl. of Jeffrey H. Schoenberg, Doc. 785-5; Decl. of Megan Missett, Doc. 640-1 at 149-154; Decl. of William Digges, III, Doc. 640-1 at 167-170; Decl. of Laura Digges, Doc. 640-1 at 162-65; Decl. of Ricardo Davis, Doc. 640-1 at 156-160.)

The Coalition Plaintiffs have presented ballot images that they assert are evidence of clear voter disenfranchisement. The 5 ballot images shown below depict actual unadjudicated ballot images from Fulton County's August 11, 2020 election, showing the ICC scanner interpreted as a "blank contest" several voter marks that indicate a clear visible selection for the candidate[78]:

1316*1316

1317*1317

(Pls.' Hrg. Ex. 7; *see also* Decl. of Marilyn Marks ¶ 17, Doc. 809-5; Ex. 19-D to Decl. of Marilyn Marks, Doc. 853-4 at 41.)

The State Defendants assert in opposition to Plaintiffs' motion that "[t]he only possible burden on a voter arising from the scanner-threshold settings is if the voter disregards the instructions that come with the ballot. That is not a burden on the right to vote — it is a voter choosing to not follow the required regulatory structure of the state." (State Defs.' Resp., Doc. 834 at 25.) In essence, the State Defendants contend that a voter who marks their absentee paper ballot with a check mark or an X, rather than filling in the oval to the left of the candidate name, does not have a right to have their vote counted. (*See* Suppl. Decl. of Chris Harvey, Doc. 834-3 ¶¶ 4-5) ("The instructions for absentee ballots instruct voters to fill in the bubble next to the preferred

candidate name and instructs voters not to make check marks or X to mark their ballot. Tabulating absentee 1318*1318 ballots where voters do not follow the instructions takes additional time for county election officials."). Defendants' litigation position, as explained below, is not in line with the requirements of Georgia's Election Code and the State Election Board's regulation providing that if the voter "has marked his or her ballot in such a manner that he or she has indicated clearly and without question the candidate for whom he or she desires to cast his or her vote, his or her ballot shall be counted, notwithstanding the fact that the elector in indicating his or her choice may have marked his or her ballot in a manner other than as prescribed."[79] Ga. Comp. R. & Reg. r. 183-1-15-.02(2)(2).

1. Operation of the Scanners

The Dominion precinct (ICP)[80] and central count (ICC)[81] scanners do not interpret the text of a hand marked paper ballot.[82] (Decl. of Dr. Eric Coomer ¶ 9, Doc. 658-2.) Instead, the scanners detect votes by reading particular coordinates on the ballot, what is known as a "target area" inside an oval next to a voter's choice as shown below:

1319*1319

(Coomer Decl. ¶ 9; Ex. A to Coomer Decl., doc. 658-2 at 9.) The target areas correlate to the voter choices represented on the ballot. (*Id.*) According to Dominion's documentation,

When a ballot is fed into an ImageCast tabulator — at the precinct level or centrally — a complete duplex image is created and then analyzed for tabulation by evaluating the pixel count of a voter mark. The pixel count of each mark is compared with two thresholds (which can be defined through the Election Management System) to determine what constitutes a vote. If a mark falls above the upper threshold, it's a valid vote. If a mark falls below the lower threshold, it will not be counted as a vote.

(Ex. M to Decl. of Harri Hursti, Doc. 809-3 at 48.) However, if a mark falls between the two thresholds, in what is known as the "ambiguous zone," it will be deemed as a "marginal mark"[83] and the ballot should be flagged for review by a vote review panel — either manually or using Dominion's vote adjudication software application. (*Id.*)

The default scanner threshold settings in Democracy Suite 5.5A for both the ICP and ICC are 12% for the low-end and 35% for the high-end. (Defs.' Hrg. Ex. 4 at 1, Doc. 887-4 at 2.) Dominion's "Democracy Suite 5.5A is not designed to register voter intent from a hand-marked ballot if the vote target area (oval to the left of the choice) is not marked in some manner" and does not meet or exceed the high-end threshold setting. (*Id.*) A visual representation of the threshold interpretation of voter marks is shown below:

1320*1320

(Doc. 809-3 at 48.)

For all elections conducted on the new Dominion voting system to date, including the June 2020 primary and August 2020 runoff elections, the ICP and ICC scanners were set to the default threshold settings. Using these default settings, when a ballot is scanned by either the ICP or ICC scanners, the scanners are programmed to interpret voter marks as follows: (a) any mark deemed by the scanner to be less than 12% darkened within the vote target areas (i.e., ovals) is designated as a blank vote for the given contest; (b) any mark deemed by the scanner to be equal to or greater than 35% darkened within the target ovals is designated as a vote for the choice associated to the target area marked; and (c) any mark deemed by the scanner to be equal to 12% or less than 35% darkened within the vote target ovals is designated as an ambiguous mark. (Defs.' Hrg. Ex. 4 at 1, Doc. 887-4 at 2.) Any ambiguous mark within a vote target oval does not count toward the vote total. (*Id.*) Instead, "[i]t is anticipated that ballots isolated by the ICP or ICC scanners containing scanner-deemed ambiguous marks are adjudicated manually or electronically by the designated election official in order to determine the voter intent that is in question by the ICP or ICC scanners." (*Id.*)

According to the Coalition Plaintiffs' expert Harri Hursti, Dominion's precinct and central count scanners cannot be relied upon to accurately count all votes using the default threshold settings and the current configuration for image resolution. (Tr. Vol. I at 125.) In addition to the use of arbitrary default threshold settings, Hursti criticizes Dominion's configuration of the ICC central count scanner to intentionally downgrade the resolution quality of the scanned image. Hursti testified that the ICC central count scanner "can be configured to capture higher quality and more information retaining images" and is capable of producing images of a significant higher order of magnitude than it currently produces based on Dominion's programming. (*Id.* at 126, 133-34.) As Hursti explained, "the way the scanner is used in this environment is like driving your sports car locked on the first gear." (*Id.* at 134.) The central count scanner is recording a lower quality image than it is capable of because "as part of the configuration, that scanner is instructed to produce low quality images with a reduced amount of 1321*1321 information." (*Id.*) For example, the image produced by the ICC is only 200 dots per inch ("DPI") which is "a fraction of what the scanner is capable" of producing and the image "has been reduced to have only black or white pixels based on algorithms and so-called business logic and the scanner itself is capable of producing color images and gray scale images." (*Id.* at 135-36.) Dominion also configured the ICC scanner to "drop out" or ignore red pigment from the scanned image. (*See* Ex. E to Hursti Decl., Doc. 809-3 at 40.) As a result, any red markings do "not meet the internal algorithm criteria for black, therefore [red] gets erased to white instead." (Hursti Decl. ¶ 61, Doc. 809-3.)

During the September 10, 2020 injunction hearing, Mr. Hursti explained that he would have expected the ICC scanner to have counted the clear voter marks shown in the ballot images of the Fulton County August 11 election interpreted by the ICC as "blank" contests. (Tr. Vol. I at 136.) The problem according to Hursti is that "the scanner is reducing all information to either black or white and that predetermination tells what the image is recording. And after that, a mathematical algorithm is applied which is only blindly counting how many black and white pixels it sees and based on that make[s] a determination if there is a vote or not. So based on that reduced information, the system didn't cross the threshold to see [those markings] as a vote or even as ambiguous mark[s]." (*Id.* at 137.) An ambiguous mark means "that the system sees something, which it says that it is not clear whether it is a mark or not. And that would have then gone to the human [ballot review] process." (*Id.* at 138.) But in the case of the Fulton County

ballot images in Plaintiffs' Hearing Exhibit 7, "the system didn't even see that there would be a mark requiring a human observation." (*Id.*)

The Coalition Plaintiffs conducted an examination of test ballots scanned on the ICP precinct scanner/tabulator using test ballots with various types of markings and different colors of pens. (*See* Pls.' Hrg. Ex. 7.1, Doc. 888-6.) Plaintiffs' Hearing Exhibit 7.1 illustrates two images of the same ballot produced by two different image resolutions and qualities and the scanner's resulting interpretation of the voter markings from the lower quality scan.[84] According to Mr. Hursti, the visible differences in the two images are "hallmarks of bad quality scanning and bad quality technology." (Tr. Vol. I at 139.) The poor quality of the ballot image scanned on the ICP does not even show the ovals that would be filled in by the voter. (*Id.*) Mr. Hursti believes that for the ICC scanner, the DPI level could be increased from the current 200 DPI configuration to 300 DPI, which is the standard setting for commercial off-the shelf scanners in order to improve the quality of the image of the ballots scanned for interpretation by the system software threshold settings.[85]

During the court-authorized testing of the Dominion equipment supplied by Fulton County, Coalition member Jeanne Dufort marked and scanned a series of test ballots to see how the marks were interpreted and tabulated by the scanner. To replicate the various ways voters might 1322*1322 feed paper ballots into the scanner, Dufort scanned the same ballot multiple times "top side up, top first and then bottom first, and bottom side up, top first, and then bottom first to see if it made any difference in how the scanner saw the vote." (*Id.* at 178.) As Dufort described at the September 10 hearing, the test ballot "had five contests on it. Three were races, and two were questions. When I put it through, the first thing I did was put it through each of the four possible ways to feed it. And each time, I got a different message from the scanner. It would return it with an error saying there were ambiguous marks, but it never pointed out the same ambiguous marks." (*Id.* at 179.) More specifically, she testified that "the first time when we put it in face up like you see first, it told us that one SPLOST race, one of the contests on the backside, was ambiguous. The second time when I put it in bottom first, it told me that the liquor sale vote was what was ambiguous and it didn't tell me anything about the SPLOST. The third time when I turned it over and put it backside facing up top end, it told me the SPLOST and one of the judge races was ambiguous. Then the fourth time when I put it backside bottom in, it told me the SPLOST and the liquor sales was in there." (*Id.*) Each of the four times Dufort fed the same ballot through the scanner, she got four different responses from the scanner. (*Id.* at 179-80.) Dufort repeated the experiment again, this time feeding the ballot in the same direction five separate times and still each time she got a different response from the scanner. (*Id.* at 180-81.)

Dr. Eric Coomer, the Director of Security for Dominion Voting Systems disagrees with Plaintiffs' contention that the Dominion scanners either discard or disregard valid votes or do not count certain marks as a vote even though the marks are obvious to the human eye as indications of a vote. (Tr. Vol. II at 73, 77.) According to Dr. Coomer, the system is simply scanning the image and detecting the percentage fill of the target area. Based on the settings, it will automatically say whether it is a valid counted vote, whether it is an ambiguous mark, or whether the system does not characterize it as any. "There are further processes in the system, mainly adjudication, which allows secondary review — voter review for voter intent issues, which is integral to the system, which is where you can apply voter intent guidelines and processes to

essentially characterize a vote that the system is not automatically specifying as a vote." (*Id.* at 73.)

During the hearing on September 11, 2020, Dr. Coomer was shown the Fulton County ballot images in Plaintiffs' Hearing Exhibit 7. Although Dr. Coomer disagrees with the contention that the scanners do not count certain marks that are visible to the human eye as votes, he admits that the mark shown by candidate Theodore "Ted" Jackson's name on the first page of Plaintiffs' Hearing Exhibit 7 looked like a vote to him but that according to the AuditMark created at the time of scanning, the ICC did not recognize the mark as a vote and did not count it as a vote. (*Id.* at 73-74.) Dr. Coomer also admitted that if a voter's mark is below the low-end threshold, it does not register as either an ambiguous mark or a vote. (*Id.* at 77.) According to Dr. Coomer's hearing testimony, the AuditMark created at the time of scanning, which contains the text indicating how the scanner interpreted the voter mark, does not indicate whether the ballot fell within the ambiguous threshold required for adjudication. (*Id.* at 75.) Therefore, one cannot tell from the AuditMark for the ballot image at page one of Plaintiffs' Hearing Exhibit 7 whether the ballot was flagged for adjudication. (*Id.*) Dr. Coomer stated that the "AuditMark simply shows everything 1323*1323 that was counted as a vote. There is additional metadata in the cast vote record, which is the electronic record, that includes information about ambiguous marks. And that is the data that is used to determine whether it is sent to adjudication." (*Id.* at 78.) But then when asked "[i]f the ballot in this particular case had been adjudicated to be a vote, would that adjudication show up on this AuditMark?," Dr. Coomer replied "Yes, it would." (Id.) And again, he was asked "if it had been adjudicated in the course of a normal election process, you would have seen that on the AuditMark in front of us; right?," Dr. Coomer responded, "Yes. Yes."[86] (*Id.* at 79.) But the AuditMark on this ballot — Hearing Exhibit 7 — did not reflect that it had been flagged for adjudication.

Dr. Coomer also disagrees with Mr. Hursti, testifying that the accuracy of the ICP and ICC scanners "has absolutely nothing to do with the scanner resolution, the DPI setting." (*Id.* at 72.) According to Dr. Coomer, because the "Dominion scanners capture the percentage fill of the targets for every mark that is made on the ballot, that has absolutely nothing to do with the scanner resolution, the DPI setting, whether a mark is characterized as a ballot vote, an ambiguous mark, or not a vote is wholly dependent on the threshold settings of the lower and upper threshold limits as well as the percentage fill of the target detected by the system." (*Id.*) He went on to "categorically state that going from the current 200 DPI to some higher level of 300 DPI does not improve the accuracy of the system." (Tr. Vol. II at 147.) Referring back to the ballot images in Plaintiffs' Hearing Ex. 7, Dr. Coomer explained that "just to put it simply, we have all seen the images. And the images clearly show the voter's mark ... if you had a physical ballot and you had some mark on there and then you showed the [scanned ballot] image and that mark wasn't there, then we could talk about DPI. But the fact is we're looking at the image. The mark is there" so the issue is "not the fact that the image is not, you know, sufficiently fine enough resolution to capture that." (*Id.* 147-48.) But, the ballot images in Plaintiffs' Ex. 7.1 show the exact scenario Dr. Coomer admits might indicate a problem with low DPI resolution. In these side-by-side images of the same ballot, the first image scanned at high resolution shows clearly the voter marks while the second image scanned on the ImageCast shows several of the voter marks having been erased by the system and some portions of the ballot printing totally distorted due to the poor image quality.

Dr. Coomer also attempted to explain why Jeanne Dufort experienced inconsistent results when she scanned the same ballot through the ICP scanner multiple times. According to Dr. Coomer, "the scanners have what is called a CIS array. It is contact image sensor array. That is what is used to actually digitize the image of the ballot. And those inherently, like all electronic systems, have some variability, plus or minus ten percent. So on one scan you could certainly have a target area that registers 12.5 percent and you round that up to 13. And on the next scan it could be 11.9 percent. There is inherent variability in all electronic systems ... that is irrespective of the resolution setting that's on the system. (Tr. Vol. II at 148-149.)

1324*1324 **2. Vote Review Panel Evidence**

The Coalition Plaintiffs presented testimony from individuals who either served on or observed vote review panels. According to Coalition member Jeanne Dufort, who testified at the September 10 hearing and serves on the adjudication panel in Morgan County, the vote review panel "makes up for the limits of technology. We take ballots that can't be scanned or ballots that have marks that the scanner can't interpret, and we put human eyes on them. So I like to think of us as backstop to make sure that every vote ... where voter intent is clear gets counted." (Tr. Vol. I at 171.) Under the new system, counties have the option to use the Dominion adjudication software to review scanned ballot images cued up on a computer screen. (*Id.*)

Adam Shirley served on the Clarke County Vote Review Panel for the June 9, 2020 Presidential Preference Primary and General Primary. (Decl. of Adam Shirley, Doc. 809-7.) Out of approximately 15,000 scanned absentee ballots, about 350 were flagged for adjudication by the software. When adjudicating a ballot, a scanned image of the complete ballot was displayed on the screen. The software indicated the flagged contests for human review by outlining them in red. The software used highlighting to indicate how it had interpreted the voter's mark. This highlighting was used for the entire ballot, not only the contests that were flagged for adjudication. Green highlighting indicated the software recognized the mark as a vote and counted it unless it was also flagged as an overvote. Yellow highlighting indicated the software categorized the mark as ambiguous and would not be counted until there was a vote review panel adjudication. When at least one oval in a contest was darkened sufficiently to be categorized as "ambiguous," the software highlighted the ambiguous option(s) in yellow, outlined the contest in red, and sent the entire ballot to an adjudication queue. Below is an example illustrative of the adjudication screen:

(Exhibit 2 to Shirley Decl., Doc. 809-7 at 12.)

The most common reason for ballots to be flagged as ambiguous was the voter 1325*1325 having marked their intent with check marks or X marks. The Clarke County review panel adjudicated vote marks categorized as "ambiguous" to count votes that were clear as to voter intent. The panel took the approach that for any votes flagged for adjudication, the vote should be counted if voter intent was clear from the on-screen image. In its review, the panel attempted to answer two questions: (1) could the voter's intent be discerned?; and (2) what was that intent? While only a simple majority was required, the bipartisan vote review panel's decision on each ballot reviewed was unanimous.

In the course of reviewing the entire ballot to inform their adjudication of flagged contests, the panel discovered clear ballot markings made by the voter that had not been highlighted by the software for adjudication. These markings were not counted as a vote (and therefore were not highlighted in green by the software) nor were they categorized as ambiguous (and therefore were not highlighted in yellow by the software). Below is the scanned image on one such marked ballot.

(Ex. 3 to Shirley Decl., Doc. 809-7 at 13.) The top and middle contests bear the red box flagging them for adjudication and yellow highlighting showing marks the software has classified as ambiguous. The bottom contest, though clearly marked by the voter, bears no red box or highlighting of any kind. This shows the software did not count that vote and was programmed not to send such a ballot to adjudication. The system seemed to simply ignore such votes.

In every instance the panel encountered where the system had not counted such votes (or flagged them for adjudication), the review panel agreed without question 1326*1326 that the voter had made their intent clear though the vote had not been counted. The panel therefore instructed the software to count the previously-ignored votes on the ballots, although the software had not flagged these particular votes for adjudication by the panel. Based on his review of hundreds of ballots, it is Shirley's opinion that it is possible that there were ballots with uncounted votes that would never be corrected by human review because no other marks on those ballots triggered flagging for adjudication.

The vote review panel expressed these concerns to elections staff, Election Director Charlotte Sosebee, and the Board of Elections. In response to these concerns, the Board of Elections ordered a pre-certification partial recount of only the absentee ballots for 5 of Clarke County's 24 precincts. The partial recount took place on June 17. The Election Board was not authorized by statute or rule to conduct a recount using any method other than what had been used for the first count. In the recount, 2,665 absentee ballots were rescanned and 76 ballots were flagged for adjudication. For those 76 ballots, the vote review panel unanimously agreed that 35 individual votes had not been counted by the software. Those votes were spread across 12 separate ballots. A Dominion technician confirmed the software was programmed to classify votes in one of three ways: a normal vote (highlighted in green), an ambiguous mark (highlighted in yellow), and an uncounted vote (which the system recognized, quantified, but was programmed not to count and not to be flagged for review).

As a voter, Shirley finds such a high rate of missed votes — nearly 16% of the adjudicated ballots — to be alarming. He also found concerning the procedures followed by the review panel in not providing a paper audit trail, not verifying the record of changes made to vote tallies, and not referencing the original ballot to determine if the low quality image was an accurate depiction of the voter-marked ballot. Shirley also found troubling that there was no attempt to reconcile the votes added to the vote tally before and after the adjudication process, leaving the opportunity for unauthorized changes to the tallies by others with access to the system.

Jeanne Dufort, served on the Vote Review Panel for the Morgan County Board of Elections and Registration for the combined Presidential Preference and General Primaries in June 2020. (Decl. of Jeanne Dufort, Doc. 809-6.) When she arrived at 8pm on June 9 for her duties, the elections

office was still in the process of opening absentee ballots. Dufort assisted the team in opening the remainder of approximately 3,000 mail ballots. Ballots were scanned from 10pm to 2am. Dufort noticed voters marking their choices in a number of ways, including filling in the oval, circling the oval, making X or check marks, and one who made smiley faces in the oval to mark their selection.

The Vote Review Panel convened on the afternoon of June 10. Morgan County used the adjudication software provided by Dominion. The Election Supervisor Jennifer Doran instructed the Dominion technician to pull up all ballots with overvote and ambiguous marks. There were about 150 out of 3,000 ballots to review. The Morgan County review panel used the same procedure described by Adam Shirley.

The first time the panel encountered a contest with no highlights (meaning it was deemed blank by the software), but with a clearly marked vote, Dufort asked the onsite Dominion technician whether that vote was counted, and he said "of course, that's a vote," and assured the panel it was counted. The panel moved on to the next ballot. This time Dufort asked the Dominion 1327*1327 technician to show her the cast vote record for the ballot. It showed "blank contest" for the race with no highlights, despite the presence of a clear vote. By unanimous agreement, the panel adjudicated that contest to show the vote, overriding the inaccurate tabulator software. The panel returned to the previous ballot and did the same. During the course of review of about 150 ballots, Dufort estimates the panel found and adjudicated about 20 votes that were clearly marked by the voters, but the software had interpreted as a "blank contest."

Dufort attended the Morgan County Election Board meeting on June 11, and spoke about her concerns as a review panel member and the need to expand the adjudication process to determine whether other votes had been rejected by the system. The Morgan County Election Board denied the motions of board member Helen Butler to expand the adjudication process to review the remaining 2,700 mail ballots to see if there were additional uncounted votes.

Coalition member Rhonda Martin observed somewhat similar adjudication procedures at the Fulton County Elections Preparation Center on August 14, 2020. (Decl. of Rhonda J. Martin, Doc. 809-4.) The adjudication process took place entirely on a low resolution black and white onscreen image, without looking at the original paper ballot. Based on her observation of the two vote review panels used by the Fulton County elections office, the panel members quickly clicked here and there and switched from one view to another as they examined the ballot images, without making a record of who approved each vote change or why the decision was made. Martin also observed that at times, the panel members appeared to almost forget to confer with one another and confirm that they agreed on the interpretation of the vote because they were so focused on operating the adjudication software.

Of the ten ballots Martin observed being adjudicated, three appeared to be completely blank with no votes marked anywhere on the ballot. The first review panel to encounter a blank ballot with no single vote shown paused to ask the Registrations Chief, Ralph Jones, what to do. After waiting for a while for Mr. Jones to finish up with the second review panel, the first review panel decided to accept the blank ballot so they could continue adjudicating other ballots. They did not request to see the original paper ballot to confirm that it was, in fact, blank. While not

impossible, Martin found it odd that a voter would go to the trouble of returning a ballot with no vote marks at all.

3. The Secretary of State's Center for Election Systems Study on Scanner Settings

When Plaintiffs filed their motion in August 2020, the State Election Board was considering proposed revisions to the regulation providing for "the definition of a vote" to designate specific settings for the ballot scanners used to tabulate optical scan ballots marked by hand. Plaintiffs' expert Harri Hursti asserted that before the State sets threshold standards for the Dominion system, extensive testing is needed to establish optimal configuration and to identify a setting that will not have the widespread effect of discarding at least some valid votes. (*See* Hursti Decl. ¶ 77, Doc. 809-3.) At that time, neither Mr. Hursti nor the Plaintiffs were aware of a study undertaken by the Center for Election Systems of the Secretary of State's Office in July of 2020 to determine "how various reductions to the default, ambiguous mark threshold setting within Democracy Suite 5.5A would impact the scanning and interpretation of ambiguously marked ballot samples" on the ICC central count 1328*1328 scanner. (Defs.' Ex. 4 at 1, Doc. 887-4 at 2.) "The examination was done in an effort to increase absentee ballot scanning efficiency and reduce the need to adjudicate ballots that reflect a clear voter intent." (*Id.*) A draft copy of the report prepared by CES's Michael Barnes was subsequently produced during expedited discovery prior to the injunction hearing.

As further explained in the draft report, CES undertook an examination to determine whether "the high-end setting of 35% is forcing election officials to review ballots that should instead be processed as marked by the ICC scanner on the initial read by the IC scanner" and counted as a valid vote. (Defs.' Ex. 4 at 2, Doc. 887-4 at 3.) Because "Democracy Suite 5.5A gives the end user the ability to adjust ambiguous mark threshold settings used by the Dominion scanners to interpret voter intent on hand-marked optical scan ballots," CES ran ballot test decks through the ICC scanner using various threshold settings. (Defs.' Ex. 4 at 1, Doc. 887-4 at 2.)

At the start of the examination, a "test deck of 100 hand-marked optical scan ballots was prepared. The instructions at the top of the ballot instruct the voter to fill in the oval next to the candidate of their choice. The filling in of the oval (vote target area) is designed to provide a clear intent for the ICC scanner to interpret." (Defs.' Ex. 4 at 2, Doc. 887-4 at 3.) To examine the various ways the scanner might interpret different marks, the testers did not fill in the vote target areas as instructed. Instead, "testers placed a variety of marks that only darkened a portion of the vote target areas" on the deck of test ballots. "Testers also used differing marking devices (i.e., blue ink, black ink, red ink, pencil, etc.) and marking pressures." On some ballots, testers marked outside the vote target area (by circling or underlining the candidate name rather than filling in the oval) "to confirm that marks [placed] outside the vote areas would not be recognized" by the scanner. (*Id.*)

Each test ballot had three contests with a total of 6 vote target areas (two ovals per contest). "Testers used the same type of variable mark within each of three contests when marking a ballot in an attempt to simulate how an individual voter would most likely mark each oval on their ballot in the same manner throughout." (*Id.*) As described in the CES draft report, the scanner will interpret a marked ballot in one of three ways: (1) Marked — the scanner will "interpret the

mark within all vote target areas on the ballot and increment vote totals and ballots cast total forward" (the mark falls above the high-end threshold and is counted as a vote); (2) Blank — the scanner "will interpret the vote area as not including a mark and would not increment vote total forward, but would increment the ballots cast forward" (the mark falls below the low-end threshold and is not counted as a vote in the vote totals); and (3) Ambiguous — the scanner will "not be able to determine marks and set the ballot aside for review" (the mark falls below the high-end threshold to count as a vote but above the low-end threshold to register as a blank). (*Id.*)

After marking the test ballots, the test deck was scanned a total of two times on an ICC scanner configured with the default low-end 12% and the high-end 35% settings. This process created two batches collected by the ICC scanner, each batch containing 100 ballots. Each batch was then loaded into Dominion's Adjudication Client application. The Adjudication Client application was set to review all ballots within the batch and isolate any ballots containing Ambiguous Marks, Blank Ballots, and Overvotes (the standard Adjudication Client settings). The testers created 1329*1329 6 criteria into which each ballot could fall under for review: (1) Marked — all contests on ballot contained a single interpretable mark; (2) 1/3 Ambiguous — one of the three contests on the ballot contained a mark requiring review; (3) 2/3 Ambiguous — two of the three contests on the ballot contained a mark requiring review; (4) Ambiguous — all three contests on the ballot contained a mark requiring review; (5) Blank Ballot — all three contests on the ballot contained no interpretable marks; and (6) Overvote — all contests on ballot contained multiple interpretable marks. (Defs.' Ex. 4 at 2-3, Doc. 887-4 at 3-4.)

Upon completing the review of each scanned batch within the Adjudication Client software, the testers documented the following results:

• Marked 53 • 1/3 Ambiguous 15 • 2/3 Ambiguous 11 • Ambiguous 12 • Blank 9 • Overvote 0

(Defs.' Ex. 4 at 3, Doc. 887-4 at 4.) A total of 47 ballots required some level of review after being processed by the ICC. The testers were concerned that nearly half of the test deck required additional review to determine voter intent.

In an effort to assess what impact a reduction in the high-end setting level would have on potential ambiguous marked ballots being registered on the ICC, testers reduced the default high-end setting 3 times: from 35% to 30%, from 30% to 25%, and finally from 25% to 20%. (Defs.' Ex. 4 at 3-5, Doc. 887-4 at 4-6.) In the third test pass, the testers ran the test deck through the scanner following the same protocol but the ICC scanner was configured with the low-end default setting of 12% but the high-end setting was reduced from 35% to 20%. (Defs.' Ex. 4, Doc. 887-4 at 5.) Using a high-end setting of 20%, testers documented the following results for each batch within the Adjudication Client software:

• Marked 70 • 1/3 Ambiguous 10 • 2/3 Ambiguous 8 • Ambiguous 1 • Blank 10 • Overvote 1

(Defs.' Ex. 4 at 4-5, Doc. 887-4 at 5-6.) With a low-end 12% and high-end 20% setting, there was a 36% reduction in the number of ballots (47 to 30) after scanning needing further review, in relation to the original default setting. (Defs.' Ex. 4 at 5, Doc. 887-4 at 6.) The adjustment of the

high-end setting down to 20% also resulted in 17 more ballots being processed as marked (an increase of 53 to 70) and voter intent being registered and tabulated without need of further review or adjudication. The reduction to 20% also resulted in a potential overvote being detected in the test deck that had previously been undetected using the higher high-end settings. This reduction in the high-end setting from 35% to 20% also decreased the number of ballots with all three contests registering ambiguous marks from 12 ballots down to 1 ballot. The reduction did not eliminate the presence of ambiguous marks, but it does appear to reduce the number of instances where the review of all contests on a ballot would be needed. (*Id.*)

In an effort to reveal if there were any additional ambiguous marks that could be detected and made available for review to users, the testers reduced the low-end threshold setting from 12% to 10% (keeping the high-end at the adjusted 20% threshold). (*Id.*) The testers ran the test 1330*1330 deck through the scanner following the same protocol described above, but the ICC scanner was configured with the low-end at 10% and the high-end at 20%. Using this configuration, testers documented the following results upon reviewing the test ballots within the Adjudication Client software:

• Marked 71 • 1/3 Ambiguous 13 • 2/3 Ambiguous 6 • Ambiguous 2 • Blank 7 • Overvote 1

(*Id.*) With the low-end 10% and high-end 20% settings, there was a 38% reduction in the number of ballots (47 to 29) after scanning needing further review, in relation to the original default setting. This configuration reduced the number of instances of ambiguous (12 to 2) and blank ballots (9 to 7) from the original default settings. Under these settings, 29 ballots remained as needing some physical review. (Defs.' Ex. 4 at 6, Doc. 887-4 at 7.) Of those 29, 7 ballots were seen by the ICC as completely blank. Upon physical review of the 7 ballots, 5 ballots contained no physical mark anywhere within the vote target oval, but did have the candidate name circled or underlined. The remaining 2 ballots seen as blank by the ICC, upon visual review, did have discernable marks within the vote target area, however, the mark was made with red ink. While it did not remove the detection of ambiguous marks or blank ballots, it does appear the combination of these settings eliminated the need to review some ballots and reduced the number of contests per ballot needing review when a ballot review was detected. (Defs.' Ex. 4 at 5, Doc. 887-4 at 6.)

During the assessment, the testers made note of whether the type and placement of marks in and around the vote target oval had an impact on the scanner's interpretation. (Defs.' Ex. 4 at 6, Doc. 887-4 at 7.) In addition to partial filling in of the vote target oval, the ICC scanner registered various types of marks, including an X, checkmark, dash, and dots, when they were placed within the vote target oval. The darker the mark within the vote target area, the easier the ICC registered the mark. These findings indicate that instructions to voters should inform the voter to fill in the oval next to the candidate name and to avoid circling, underlining, or placing checkmarks or Xs, or otherwise marking the candidate name outside the vote target oval. Voters should also be warned to NOT use red ink.

4. Georgia's Election Code and Regulations Pertaining to Optical Scan Ballots

Based on the results of the CES study in July 2020, the State Election Board proposed a rule adopting the adjusted threshold settings that was. The regulation, approved by the Board on September 10, 2020 now provides:

Ballot scanners that are used to tabulate optical scan ballots marked by hand shall be set so that:
1. Detection of 20% or more fill-in of the target area surrounded by the oval shall be considered a vote for the selection;
2. Detection of less than 10% fill-in of the target area surrounded by the oval shall not be considered a vote for that selection;
3. Detection of at least 10% but less than 20% fill-in of the target area surrounded by the oval shall flag the ballot for adjudication by a vote review panel as set forth in O.C.G.A. 21-2-483(g). In reviewing any ballot flagged for adjudication, the votes shall be counted if, in the opinion of the vote review panel, the 1331*1331 voter has clearly and without question indicated the candidate or candidates and answers to questions for which such voter desires to vote.

Ga. Comp. R. & Regs. 183-1-15-.02(2)(k).

The State Election Board's regulation providing for the definition of a vote, states that for optical scan paper ballots, the voter must "fill in the oval" to mark their vote choice. Ga. Comp. R. & Regs. 183-1-15-.02(2)(2)(a). Where an optical scan ballot marked by hand has been rejected by the scanner/tabulator as containing an overvote in accordance with O.C.G.A. § 21-2-483(g), in reviewing such a ballot: (1), if "it appears that there is a properly cast vote and what is clearly a stray mark which has caused the ballot scanner to read the vote for such office as an overvote, the properly cast vote shall be counted and the stray mark shall be ignored;" and (2) if "a voter marks his or her ballot in a manner other than that specified by law and this rule, the votes shall be counted if, in the opinion of the vote review panel as provided in O.C.G.A. § 21-2-483(g)(2)(B), the voter has clearly and without question indicated the candidate or candidates and answers to questions for which such voter desires to vote." Ga. Comp. R. & Regs. 183-1-15-.02(2)(2)(c)&(d). Under O.C.G.A. § 21-2-483(g)(1), "[t]he central tabulator shall be programmed to reject any ballot, including absentee ballots, on which an overvote is detected and any ballot so rejected shall be manually reviewed by [a] vote review panel ... to determine the voter's intent as described in subsection (c) of Code Section 21-2-438." O.C.G.A. § 21-2-438(c) in turn provides that "if the elector has marked his or her ballot in such a manner that he or she has indicated clearly and without question the candidate for whom he or she desires to cast his or her vote, his or her ballot shall be counted and such candidate shall receive his or her vote, notwithstanding the fact that the elector in indicating his or her choice may have marked his or her ballot in a manner other than as prescribed by this chapter."

Similarly, "[i]f, in reviewing an optical scan ballot marked by hand, a discrepancy is found between the voter's mark on the ballot that clearly and without question indicated the voter's intent and the result tabulated by the ballot scanner, the voter's mark shall control and be counted." Ga. Comp. R. & Regs. 183-1-15-.02(2)(2)(e). Finally, "[w]hen an optical scan ballot marked by hand contains stray marks or marks which prevent the ballot scanner from properly recording valid votes as determined under this rule and by law, the ballot shall be duplicated in accordance with law to correct such problems and the duplicate shall then be tabulated." Ga. Comp. R. & Regs. 183-1-15-.02(2)(2)(f). The regulation further provides that "[n]othing herein

shall be deemed to disallow the use of ballot scanners for tabulation of ballots." Ga. Comp. R. & Regs. 183-1-15-.02(2)(2)(e).

5. Plaintiffs' Proposed Remedy

Coalition Plaintiffs seek from this Court "[a]n order commanding the State Defendants to standardize required settings of Dominion precinct and central ballot scanners and related tabulation software to ensure that all perceptible votes written on mailed and hand marked paper ballots are either counted as votes or flagged for human review by a Vote Review Panel, and requiring that Dominion scanner sensitivity settings and tabulation software be uniform across all counties." (Mot., Doc. 809 at 2). According to their motion, the full problem with the ballot scanners will not be solved by the State's new rule, but it can be solved by restraining the State from requiring scanner settings that automatically discard any degree of perceptible voter markings. In response, the State Defendants 1332*1332 assert that Plaintiffs do not propose any solution beyond ensuring every single stray mark on every hand-marked ballot is reviewed by a human.

For the reasons that follow, the court will not grant the requested relief for the November general election based on pragmatic timing considerations where absentee voting has already begun and alteration of the scanner settings would require changes to the election system database and would result in disruption of the ongoing administration of the election by the State and the Counties. Instead, the Court has directed the State to itself explore and determine whether a solution exists for the discounting of votes resulting from system deficiencies in the tabulator/scanning and the potential implementation of remedial measures in time for any runoffs in January 2021.

There is no question that the default scanner settings used in elections conducted to date on the Dominion system caused certain voter marks to register as blank and therefore prevented some valid votes on hand-marked ballots from being counted. (*See* ballot images at Doc. 809-5.) The testimony of the vote review panelists clearly establish the differences between the scanner's perception and human perception of voter intent. In addition, the ballots provided in the record show that different results were reached by the scanners and the vote review panel members about whether voter markings counted. Dr. Coomer acknowledged that the scanners will not count marks that fall below the low-end threshold setting. It is also evident that the State's adjustment of the Dominion default settings (used to date) pursuant to the SEB's newly promulgated regulation will not cause the scanner software to capture all perceptible ballot vote markings and count them as votes in the upcoming November election. (*See* Defs.' Ex. 4 at 6, Doc. 887-4 at 7) (noting that even after the adjustment, 7 out of 100 test ballots were seen by the ICC as completely blank though voter markings could be discerned upon physical human review).

The scanners are programmed to flag overvotes[87] for review and adjudication. They are not, however, programmed to flag undervotes (i.e., blank contests) for review. As evidenced by the Fulton County ballots shown in Plaintiffs' Exhibit 7, the result is that some votes are not recorded by the scanners and are not counted. Under the current procedures used with the Dominion system, these votes escape any review before being rejected — resulting in irreversible voter

disenfranchisement.[88] It appears that prior to the use of the Dominion system and introduction of the adjudication software, no voter's ballot choices were getting kicked out based on their visible designations of candidate choices with an X or check mark, as these markings are recognized under Georgia's Election Code as clear manifestations of voter intent. These circumstances are quite troubling and present an opportunity to potentially disenfranchise older voters in particular — based on their historical experience voting under the State's prior systems — at a greater percentage than younger voters.

To decide whether Plaintiffs have established a substantial likelihood of prevailing 1333*1333 on the merits of their claim related to the scanner settings, the Court must first "consider the character and magnitude of the asserted injury to the rights protected by the First and Fourteenth Amendment." *Anderson*, 460 U.S. at 789, 103 S.Ct. 1564. The Court must then "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*, 520 U.S. at 358, 117 S.Ct. 1364.

Here the asserted injury is that Plaintiffs and other absentee mail voters face a risk of suffering a diminished ability to participate fully in the democratic process and to elect the candidates of their choosing if the scanners do not recognize their ballot markings as valid votes. To echo the late Congressman John Lewis, "The vote is precious. It is the most powerful non-violent tool we have in a democratic society, and we must use it." As this Court has repeatedly recognized in this case, "[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. 533, 555, 84 S.Ct. 1362, 12 L.Ed.2d 506 (1964). This right carries with it the right not only to cast a ballot but to have it counted. *United States v. Classic*, 313 U.S. 299, 315, 61 S.Ct. 1031, 85 L.Ed. 1368 (1941); *Democratic Exec. Comm. of Florida v. Lee*, 915 F.3d at 1315 ("of course, voting alone is not enough to keep democracy's heart beating. Legitimately cast votes must then be counted"). The loss of a vote cast is permanent.[89] The significance of the indelible nature of the injury cannot be overstated.

It is precisely because of the character and magnitude of the interest at stake that voters themselves have an independent responsibility to proceed with care and caution when exercising the franchise. Georgia has implemented a voting system that relies on the efficiencies afforded by technology. The State Election Board has adopted a regulation for processing and tabulating hand marked ballots using optical scanners that requires the voter to "fill in the oval" to mark their vote choice. Ga. Comp. R. & Regs. 183-1-15-.02(2)(a). Under the regulation, markings that trigger "detection of 20% or more fill-in of the target area surrounded by the oval shall be considered a vote for the selection," while markings that trigger "detection of less than 10% fill-in of the target area surrounded by the oval shall not be considered a vote for that selection." Ga. Comp. R. & Regs. 183-1-15-.02(2)(k). The burden on voters to read and follow the instructions for marking their absentee, provisional, or emergency ballots is minimal.[90] The burden to do so in a manner consistent 1334*1334 with the regulation's adopted scanner settings to ensure their vote is automatically accepted by the scanner software is a different matter. Certain well-informed voters may be aware of this new regulation adopted just weeks ago. Other voters may have read recent news articles documenting the problems with Georgia's scanners in failing to recognize certain types of voter markings during the June primary elections. The average voter,

however, is likely unaware that their failure to adequately darken the oval to a certain percentage may cause their vote to be rejected by the scanner and in turn, not counted altogether. The Court therefore finds this burden to be more than minimal but less than severe and will apply an intermediate level of scrutiny.

The Court must weigh the burden on the right to vote against "`the precise interests put forward by the State as justifications for the burden imposed by its rule,' taking into consideration the `extent to which those interests make it necessary to burden the plaintiffs rights.'" *Burdick*, 504 U.S. at 434, 112 S.Ct. 2059 (quoting *Anderson*, 460 U.S. at 789, 103 S.Ct. 1564); *see also* *People First of Alabama v. Sec'y of State for Alabama*, 815 Fed.Appx. 505, 512 (11th Cir. 2020) (Rosenbaum, J. & Pryor, J., concurring) ("But whatever the burden, no matter how slight, `it must be justified by relevant and legitimate state interests sufficiently weighty to justify the limitation.'") (internal citations omitted).

State Defendants assert that any burden on the right to vote created by the 10% threshold for discarding voter marks is justified by the regulatory interests of the State as outlined by the Secretary of State's Director of Elections, Chris Harvey. Mr. Harvey attested that "[r]equiring a manual review of every stray mark that happens to be in a target area would require significant time by county officials and would result in delays of finalizing results, certifying results, and conducting audits." (Decl. of Chris Harvey, Doc. 834-3 ¶ 9.) According to Harvey, "[u]sing a 10% threshold for scanners minimizes the burden on election officials while still ensuring that ambiguous marks are properly evaluated." (*Id.* ¶ 10.)

The Court understands that the State does not want to make the standard so low that it sweeps in thousands of ballots with actual blank contests and some truly errant marks for adjudication panel review because it might lead to an unreasonably inefficient process and become potentially unmanageable in the timeframe permitted under Georgia law for finalizing the results of the election. However, there is no evidence in the record of any burden on the Counties were the Court to grant some form of relief to address the ballot scanner settings. No evidence has been presented from any county election official to support Mr. Harvey's supposition that changes to the scanner, tabulation, and adjudication software to ensure that all perceptible votes written on mailed and hand marked paper ballots are either counted as votes or flagged for human review by a Vote Review Panel would create an undue administrative burden on county officials and would "result in delays of finalizing results, certifying results, and conducting audits." And notably, Fulton County's response to Plaintiffs' motion is silent on the issue of the ballot scanner settings.

Each county election superintendent must certify the county's consolidated election results not later than 5:00 P.M. on the second Friday following the date of the election (i.e., Friday, November 13, 2020) and immediately transmit the certified returns to the Secretary of State, "provided, however, that such certification date may be extended by the Secretary of State in his or her discretion if necessary to complete 1335*1335 a precertification audit." O.C.G.A. § 21-2-493(k). The Secretary of State must certify the election results not later than 5:00 P.M. on the seventeenth day following the date of the election, in this year that date falls on Thursday, November 20, 2020. O.C.G.A. § 21-2-499(b). Prior to final certification, Georgia's election code requires the Secretary of State "[u]pon receiving the certified returns of any election from the

various superintendents ... shall immediately proceed to tabulate, compute, and canvass the votes cast," prior to certifying the returns. *Id.* § 21-2-499(a). "In the event an error is found in the certified returns presented to the Secretary of State or in the tabulation, computation, or canvassing of votes ... the Secretary of State shall notify the county submitting the incorrect returns and direct the county to correct and recertify such returns. Upon receipt by the Secretary of State of the corrected certified returns of the county, the Secretary of State shall issue a new certification of the results." *Id.*

Under these provisions, the counties have ten days to tabulate and certify their results to the Secretary of State,[91] who in turn has an additional seven days to certify the election after a thorough review of the returns. The State Defendants' fear of an unsupported and unquantified "delay" in certification caused by review of additional ballots by a Vote Review Panel is outweighed by the burden on voters. *See* *Common Cause Georgia v. Kemp*, 347 F. Supp. 3d 1270 (N.D. Ga. 2018) (rejecting the State's argument that remedy requiring measures to ensure proper counting of provisional ballots would delay certification of election under statutory timeline for certification); *Doe v. Walker*, 746 F. Supp. 2d 667, 678-80 (D. Md. 2010) (finding that Maryland's statutory deadline for the receipt of absentee ballots imposed a severe burden on the absent uniformed services and overseas voters that was not justified by the state's interest in certifying election results).

The Court finds that Plaintiffs have satisfied the first two prerequisites for preliminary injunctive relief. Plaintiffs have presented enough evidence to establish a substantial likelihood of success on the merits of their claim that the State Defendants' use of an arbitrary threshold on its ballot scanners to discard voter ballot markings for specific candidates or initiatives that are obvious to the human eye results in a violation of the fundamental right of each voter to have his or her vote accurately recorded and counted. *See* *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 451, 128 S.Ct. 1184, 170 L.Ed.2d 151 (2008) (holding that state and local laws that unconstitutionally burden the right to vote are impermissible); *Democratic Exec. Comm. of Florida v. Lee*, 915 F.3d at 1321 (characterizing disenfranchisement by signature mismatch rules as imposing a serious burden on the right to vote); *League of Women Voters of N.C. v. North Carolina*, 769 F.3d 224, 244 (4th Cir. 2014) ("[E]ven one disenfranchised voter—let alone several thousand—is too many.") The threat of this injury is substantial and irreparable if relief is not granted before the election. *See* *Elrod v. Burns*, 427 U.S. 347, 373, 96 S.Ct. 2673, 49 L.Ed.2d 547 (1976) (plurality opinion) (The "loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury."); *Martin v. Kemp*, 341 F. Supp. 3d 1326, 1340 (N.D. Ga. 2018) ("The Court finds that [p]laintiffs have established irreparable injury 1336*1336 as a violation of the right to vote cannot be undone through monetary relief and, once the election results are tallied, the rejected electors will have been disenfranchised without a future opportunity to cast their votes."); *see also* *League of Women Voters of N.C.*, 769 F.3d at 247 ("Courts routinely deem restrictions on fundamental voting rights irreparable injury... [because] once the election occurs, there can be no do-over and no redress. The injury to these voters is real and completely irreparable if nothing is done to enjoin the law.").

The Court must now consider the requested relief in connection with the two remaining requirements for granting a preliminary injunction: whether the threatened injury to the Plaintiffs outweighs the harm an injunction may cause the Defendants and whether granting the injunction

is in the public interest. The Court considers these last two factors "in tandem ... as the real question posed in this context is how injunctive relief at this eleventh-hour would impact the public interest in an orderly and fair election, with the fullest voter participation possible...." *Curling v. Kemp*, 334 F. Supp. 3d 1303, 1326 (N.D. Ga. 2018), *aff'd in part, appeal dismissed in part*, 761 F. App'x 927 (11th Cir. 2019); *see also Purcell v. Gonzalez*, 549 U.S. 1, 4, 127 S.Ct. 5, 166 L.Ed.2d 1 (2006). Indeed, the Supreme Court has recognized that there are special considerations involved with impending elections and the critical issues at stake. In *Reynolds v. Sims*, the Court stated:

[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.

377 U.S. at 585, 84 S.Ct. 1362. The Court notes, however, that *Reynolds* is not an inviolable commandment against pre-election injunctions where the constitutional violations are significant, and the relief is not adverse to the public interest.

Plaintiffs' requested relief is based on proposed solutions of their cybersecurity and scanner expert, Harri Hursti.

First, in his August 24, 2020 declaration, Mr. Hursti called for extensive testing before choosing mandated threshold settings. The Secretary of State's Center for Election Systems conducted an assessment of various scanner settings before landing on the low-end 10% and high-end 20% threshold settings. But the CES did not test or assess thresholds lower than 10%. CES's assessment resulted in a significant increase in the number of marks recognized by the ICC as valid votes and a corresponding decrease in the number of marks characterized as blank votes as well as significant decrease in the number of marks flagged as ambiguous requiring further adjudication. Despite this notable improvement, this one adjustment alone does not address the outstanding injury experienced by a significant number of voters who cast hand marked ballots (and votes) that will continue to be excluded from "counting" although they manifest the voter's 1337*1337 electoral designation intent. Based on the results of the CES study as well as other evidence in the record, clearly evident ballot vote markings will not be detected by the Dominion tabulators, and such marks will not be counted as votes absent further exercise of human judgment in review of improved images of the ballots or the original ballots or alternatively, improved screening by the adjudication software. While the precise scope of the affected ballots is unknown, the evidence reviewed indicates that there remains a sufficient volume of impacted voters post implementation of the State's new 10% bottom threshold rule, that these incidents are not errant, isolated cases that can be simply ignored as the incidental vote counting errors or irregularities that can be expected in a large election. Nor are they just "incidental" or accidental "errors" to the extent that the software operates to exclude voting

marks that clearly manifest the intent of the voter and therefore must be considered as a vote under Georgia law.

Second, for the ICC central count scanner Mr. Hursti proposes that the current configuration be modified "to allow the scanner to capture the images with a higher resolution and higher amount of information, meaning either color or gray scale images" and to adjust the DPI from 200 to the "current minimum standard of office technology" of 300 DPI.[92] (Vol. I at 143.) He recommends as a stop-gap measure and mitigation for the November 2020 election that the State undertake an examination of the necessary changes to ensure that every vote is counted. (*Id.* at 161-62.)

As previously discussed, Dr. Coomer testified, scanner threshold settings for the Dominion Democracy Suite 5.5-A are not set on each individual scanner. Instead, scanner threshold settings are set when the voting database is built. (Tr. Vol II at 83.) While Dr. Coomer acknowledged that the settings on the central count scanners could be changed before the project is 1338*1338 built, he stated that as of September 11, 2020, Dominion is in the midst of building the project for the November election. (*Id.* at 84.)

Accordingly, the Court must consider remedies that go beyond the 10 to 20 percent threshold standard recently adopted by the Secretary of State, while balancing the potential for administrative confusion and serious vote mishaps by any course of action that is not deliberate and properly researched. The Court is not prepared to direct the State to make additional adjustments to the settings prior to the November election because it is not feasible under the circumstances where the voting database has already been built, has been rolled out to the counties, and has already or soon will be undergoing logic and accuracy testing. There are additional challenges of implementing manageable relief where the evidence is not clear that the resolution can be fixed on the software in time or moreover, whether a software fix of ballot image resolution quality would be effective or not in increasing the number of ballot markings that will be automatically read and counted as votes by the scanner/tabulators.

The current adjustments of the default settings adopted by the State in time for the November election lowers the gateway and allows more paper ballots with voter marks such as Xs or checks (rather than oval fill-ins) to be counted or referred for adjudication of voter intent. This change in settings used in the 2019 pilots and the 2020 primary elections, while an incomplete remedy, should be an improved mechanism to address the issue of lost scanned hand marked ballot votes in the voting tabulation in the November election. Plaintiffs as well as the Defendants or County Boards of Election may of course revisit the question of additional relief related to the ballot scanners if there turns out to be more evidence after the election and if huge swaths of voters' absentee, provisional, or emergency paper ballot votes did not count.[93]

That said, the evidence supports a finding that the modified scanner settings may well still result in the rejection of valid votes and ballots falling through the identified crack in the system by failing to flag visibly clear voter marks for adjudication by a review panel. Although the Court will not require further changes to the scanner settings prior to the November election, another potential measure may allow for an expanded review of optical scan hand-marked ballots in connection with the adjudication software. Ballot contests flagged for human review by the adjudication software appear on the review screen with a red box outline around the contest. The

adjudication software assigns green high-lighting to voter marks that meet the high-end threshold setting to count as a vote and assigns yellow highlighting to voter marks that fall between the high and low-end threshold settings and deemed by the scanner as ambiguous. Currently, the adjudication software does not assign any high-lighting to voter marks that are deemed blank because they fall under the low-end threshold setting.[94] Because the adjudication software is capable of isolating ballot marks flagged as ambiguous, it would 1339*1339 make sense that the software could similarly be configured to isolate ballot marks interpreted as "blank." It therefore appears likely that the adjudication software can be used to review ballot images flagged with blank contests to verify that no clearly discernable ballot marks are present on the ballot images that have not been recognized by the scanner software as falling within the designated threshold to constitute a vote.[95] As the vote review panel testimony indicates, the adjudication software allows the reviewer to quickly scan and move through the flagged ballot images on the review screen.[96] The Court recognizes the potential for a large number of ballots with truly blank contests (those where a voter intentionally chose not to mark a vote for a particular candidate or ballot question) are swept in for review. For this reason, a thorough examination of the feasibility of using the adjudication software for this purpose may reveal that any material increase in burden on election officials to perform this additional review measure weighs against its consideration as a potential method of relief in future elections after November.

Accordingly, the Court GRANTS relief that is narrowly tailored to address the specific voter disenfranchisement by operation of the optical scanners/tabulators in tandem with the BMD adjudication software raised in Plaintiffs' motion. The Court finds that injunctive relief is warranted but based on the testimony and evidence in the record, recognizes that there will not be an "instant fix" of this issue, though in any event, remedial measures should be in place by the next election cycle following the January 2021 election cycle, or if feasible, by the January 2021 runoff elections.

The Court has reviewed the Coalition Plaintiffs' requested relief (Docs. 809, 817) and finds that the relief identified is at once broader than what is called for to address the specific injury identified[97] and on the other hand, insufficiently precise. Accordingly, the Court DIRECTS Plaintiffs to submit a proposed injunctive relief order that delineates the specific measures or course of action they are seeking that the Court adopt to address this vote counting issue by October 26, 2020. In that connection the Court recognizes the State Election Board and Secretary's staff and/or Plaintiffs may likely need to conduct a further review with Dominion and other potential experts of some additional 1340*1340 suitable options to address the issues raised here and to run sample tests to further assess such options; to consider the remedy of red outlined vote target ovals on hand marked ballots as used in other jurisdictions contracting with Dominion that facilitate the reading of a fuller range of voter markings; and the schedule for proceeding if programming changes must be made to implement the chosen option(s) in conjunction with the build of the ballot database for the election in question, as Dr. Coomer indicated would be necessary for some changes. This is how Dominion proceeded with the build of the database for the current election while a proposed regulation for modified threshold percentages was pending before the State Election Board.

In a rational world, the parties' representatives would sit down and discuss these matters together to discuss alternative remedial courses of action and further review. The Court would be more

than willing to facilitate this by modifying timelines. In any event, the expanded method(s) to address the scanner/tabulator and adjudication software's per se "blank" exclusion of marks that may reasonably be considered by an adjudication panel as indicating voter intent must be in place no later than the next election cycle following the conclusion of the January 2021 runoffs. The Court will enter a further relief order upon receipt of Plaintiffs' proposed remedy by October 26, 2020 and Defendants' response within 14 days of receipt of the Plaintiffs' proposal.

IV. Conclusion

The Constitution's preamble speaks first of "We, the People," and then of their elected representatives. The judiciary is third in line and it is placed apart from the political fray so that its members can judge fairly, impartially, in accordance with the law, and without fear about the animosity of any pressure group.
In Alexander Hamilton's words, the mission of judges is "to secure a steady, upright, and impartial administration of the laws." I would add that the judge should carry out that function without fanfare, but with due care. She should decide the case before her without reaching out to cover cases not yet seen. She should be ever mindful, as Judge and then Justice Benjamin Nathan Cardozo said, "Justice is not to be taken by storm. She is to be wooed by slow advances."[98]

Plaintiffs' challenge to the State of Georgia's new ballot marking device QR bar-code-based computer voting system and its scanner and associated software presents serious system security vulnerability and operational issues that may place Plaintiffs and other voters at risk of deprivation of their fundamental right to cast an effective vote that is accurately counted. While these risks might appear theoretical to some, Plaintiffs have shown how voting equipment and voter registration database problems during the 2019 pilot elections and again in the June and August 2020 primary elections caused severe breakdowns at the polls, severely burdening voters' exercise of the franchise. (*See* September 28, 2020 Order, Doc. 918.)

Established Supreme Court authority recognizes that States retain the authority and power to regulate their elections and the voting process itself, subject to the preservation of citizens' fundamental First and Fourteenth Amendment rights. And the Supreme Court has repeatedly emphasized in the last months the principle that 1341*1341 district courts must exercise great restraint in considering the grant of injunctive relief that requires major new electoral rules on the cusp of an election where a court's order could cause electoral disruption and potential voter confusion. The posture of this case collides with this latter principle. The sweeping injunctive relief that Plaintiffs seek would require immediate abandonment of the ballot marking device voting system enacted by the Georgia Legislature in 2019 that is in its first year of implementation by the Secretary of State pursuant to his authority under Georgia law. Though major difficulties have arisen during the course of this new system's rocky first year, the Court recognizes that the staff of the Secretary of State's Office and county election offices have worked hard to roll out the system in short order during a Covid-19 pandemic era that presents unique hurdles. That hard work though does not answer the fundamental deficits and exposure in the system challenged by Plaintiffs.

Thus, although Plaintiffs have put on a strong case indicating they may prevail on the merits at some future juncture, the Court must exercise real caution in considering the grant of their

request for extraordinary injunctive relief, given its obligation to follow governing Supreme Court and Eleventh Circuit authority. Despite the profound issues raised by the Plaintiffs, the Court cannot jump off the legal edge and potentially trigger major disruption in the legally established state primary process governing the conduct of elections based on a preliminary evidentiary record. The capacity of county election systems and poll workers, much less the Secretary of State's Office, to turn on a dime and switch to a full-scale handmarked paper ballot system is contradicted by the entire messy electoral record of the past years. Implementation of such a sudden systemic change under these circumstances cannot but cause voter confusion and some real measure of electoral disruption. As with any systemic change, implementation of a statewide handmarked paper ballot system as the State's primary electoral system would require long term planning and advanced poll worker training. Accordingly, based on the binding appellate legal authority, the State's strong legal interest in ensuring an orderly and manageable administration of the current election, and the Court's assessment of the operational realities before it, the Court must deny the Plaintiffs' Motions for Preliminary Injunctive Relief in so far as they request immediate replacement of the current BMD system with a statewide hand-marked paper ballot system.[99]

But the Court cannot part with that message alone. The Court's Order has delved deep into the true risks posed by the new BMD voting system as well as its manner of implementation. These risks are neither hypothetical nor remote under the current circumstances. The insularity of the Defendants' and Dominion's stance here in evaluation and management of the security and vulnerability of the BMD system does not benefit the public or citizens' confident exercise of the franchise. The stealth vote alteration or operational interference risks posed by malware that can be effectively invisible to detection, whether intentionally seeded or not, are high once implanted, if equipment and software systems are not properly protected, implemented, and audited. The modality of the BMD systems' capacity to deprive voters 1342*1342 of their cast votes without burden, long wait times, and insecurity regarding how their votes are actually cast and recorded in the unverified QR code makes the potential constitutional deprivation less transparently visible as well, at least until any portions of the system implode because of system breach, breakdown, or crashes. Any operational shortcuts now in setting up or running election equipment or software creates other risks that can adversely impact the voting process.

The Plaintiffs' national cybersecurity experts convincingly present evidence that this is not a question of "might this actually ever happen?" — but "when it will happen," especially if further protective measures are not taken. Given the masking nature of malware and the current systems described here, if the State and Dominion simply stand by and say, "we have never seen it," the future does not bode well.

Still, this is year one for Georgia in implementation of this new BMD system as the first state in the nation to embrace statewide implementation of this QR barcode-based BMD system for its entire population. Electoral dysfunction — cyber or otherwise — should not be desired as a mode of proof. It may well land unfortunately on the State's doorstep. The Court certainly hopes not.

The Court recognizes the major challenges facing the Secretary of State's Office in rapidly implementing a new statewide voting system. Yet the vital issues identified in this case will not

disappear or be appropriately addressed without focused State attention, resources, ongoing serious evaluation by independent cybersecurity experts, and open-mindedness. The Secretary of State and Dominion are obviously not without resources to tackle these issues. And at very least, the Court cannot fathom why, post-election, the State and Dominion would not at least be moving toward consideration of the software upgrade option Dominion originally promised, allowing voters to cast ballots that are solely counted based on their voting designations and not on an unencrypted, humanly unverifiable QR code that can be subject to external manipulation and does not allow proper voter verification and ballot vote auditing.

Time will tell whether Act V here can be still avoided or at least re-written.

For the foregoing reasons, the Court DENIES the Curling Plaintiffs' Motion for Preliminary Injunction [Doc. 785] and DENIES IN PART AND GRANTS IN PART the Coalition Plaintiffs' Motion for Preliminary Injunction on BMDs, Scanners, and Tabulators, and Audits [Doc. 809].

IT IS SO ORDERED this 11th day of October, 2020.

[1] The two sets of Plaintiffs in this case are represented by separate counsel and seek overlapping but somewhat differently articulated, equitable relief. Donna Curling, Donna Price, and Jeffrey Schoenberg are referred to as the "Curling Plaintiffs." The Coalition for Good Governance ("Coalition"), Laura Digges, William Digges III, Ricardo Davis, and Megan Missett are referred to as the "Coalition Plaintiffs."

[2] *See* O.C.G.A. § 21-2-300(a)(2); O.C.G.A. § 21-2-2(7.1); O.C.G.A. § 21-2-300(a)(2); Ga. Comp. R. & Reg. r. 590-8-1-.01(d).

[3] The Court summarized the three-year background history surrounding this case in its Order of August 7, 2020 (Doc. 768) that denied without prejudice Plaintiffs' earlier facial challenge of the BMD system, filed in October 2019, before any elections using the system had been held.

[4] Plaintiffs in this connection present evidence of the votes on some hand-marked ballots being treated as blank votes because the optical scanner failed to recognize the hand-made mark that did not fully fill in the vote bubble, although the hand votes still demonstrated the voter's ballot intent through a check or X or otherwise, and therefore would satisfy the requirement of Georgia law for being counted. The State Board of Elections has recently approved some modifications in the scanning program settings that may result in more of these "blank" votes being flagged and referred to county adjudication panels for review. The Coalition Plaintiffs have offered expert testimony that other scanner adjustments can be made that would more completely address this ballot scanning issue. Defendants dispute this.

[5] Dominion Voting Systems, Inc.'s contract with the Georgia Secretary of State calls for Dominion's provision of all equipment and software components of the BMD system as well as training and technical assistance. (Doc. 786.)

[6] As detailed in the Court's Order of September 28, 2020, Plaintiffs' challenge also addresses dysfunctions in the voter registration information database system and the pollbook voter check-in system, both of which they contend fundamentally impact the voting process and voter access to the ballot. (Doc. 918.)

[7] Although Defendant Fulton County has also taken an active role in the defense of this litigation the State Defendants' counsel have assumed by far the primary role in presentation of the defense. Representatives of both the State Defendants and Fulton County at various points have acknowledged some of the genuine challenges and major problems experienced in the first statewide in person election for a large array of offices that was held on June 9, 2020 using the new BMD system. (The March 24, 2020 presidential primary election was postponed twice — once

until May 19, 2020 and then until June 9, 2020. Some voters cast absentee mail ballots and absentee in-person "early voting" ballots before the March primary was postponed.)

[8] *See generally*, O.C.G.A. § 21-2-384, § 21-2-385(a); *see also* Georgia Secretary of State's web posting, Elections and Voter Registration Calendar, https://sos.ga.gov/admin/files/2020%20Revised%20Short%20Calendar.pdf (last visited September 17, 2020).

[9] As found in the Court's 2018 and 2019 Orders, the Secretary of State contracted with Kennesaw State University from 2002 to December 2017 to maintain the central server and provide critical related election services for the State at a unit in the University called the Center for Election Services ("CES"). Evidence reviewed in detail by the Court showed that the central server was accessible via the internet from at least between August 2016 and March 2017. After an information security engineer KSU's Information Security Office performed a scan of the server on March 4, 2017, it was immediately taken down. The FBI was contacted and took temporary possession of the elections server. Prior to returning it to KSU, the FBI made two forensic images of the server. KSU destroyed the original server and backup server soon after the news of the breach was publicized and after Plaintiffs' lawsuit was served on Defendants.

[10] *Curling v. Kemp*, 334 F.Supp.3d 1303 (N.D. Ga. 2018).

[11] The leadership of the Secretary of State's Elections Division and Center for Elections Systems (transferred from Kennesaw) has remained intact throughout.

[12] Dr. Wenke Lee, Professor of Computer Science at Georgia Tech University and Co-Executive Director of the Institute for Information Security, was the sole computer scientist appointed to the Secretary of State's Secure Accessible Fair Elections ("SAFE") Commission.

[13] In 2019, South Carolina began using the ExpressVote ballot marking system developed and marketed by ES&S.

[14] Warren Stewart is a Senior Editor and Data Specialist at Verified Voting.

[15] *See* Verified Voting, The Verifier, https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020 (last visited Aug. 18, 2020). (*See also* Ex. 1 to Stewart Decl., Doc. 681-2 at 6-14.)

[16] "Clarification Questions*MS 16-1 Supply Chain Dominion and KnowInk Final.docx" *available at* https://sos.ga.gov/admin/uploads/Dominion.zip.

[17] EAC is the acronym for the U.S. Election Assistance Commission.

[18] Other manufacturers offer EAC-certified non-barcode BMDs, including the Clear Ballot ClearAccess system and the Hart Verity Touch Writer. Instead of a barcode for vote tabulation, these systems print a ballot that looks like a hand-marked paper ballot but has scan targets filled in for the selected candidates. (Decl. of Dr. Alex Halderman, Doc. 785-2 ¶ 37.)

[19] If the referenced Dominion software upgrade moved forward and was purchased, this would also allow an independent audit's capacity to track voting back to scanned ballots that are counted by a scanner based on human text identified voter selections that serve as the actual basis for the scanner/tabulators' tallying of ballot votes.

[20] For a variety of reasons, local precinct polling stations end up sending emergency ballots to their Counties' election office for scanning and tabulation rather than handling this themselves. Local precincts in the past have treated emergency ballots like provisional ballots that must be sent to the County office for a determination to be made of voter eligibility. However, consistent with current state regulations, precincts processing emergency ballots

are authorized to allow voters to cast and scan their own emergency ballots, assuming voting equipment is operational.

[21] State Defendants requested that some of the Plaintiffs' expert testimony be presented in sealed proceedings and affidavits to ensure the protection of Dominion's intellectual property and the security of the voting system. The Court preliminarily granted these requests by and large so as to rapidly move proceedings forward as it could not predict precisely what matters would be covered in the testimony or the import of information in advance. Plaintiffs preserved their objections to the sealing. The Court will reconsider these sealing decisions, if appropriate, upon a properly supported motion.

[22] According to Mr. Cobb's first affidavit, "Georgia certified the Dominion Voting's Democracy Suite 5.5-A in August 2019. Pro V&V did not test this specific version of the voting system for the EAC, but had previously engaged in testing the baseline system (D-Suite 5.5)," apparently for another client. (Doc. 821-6 at 3-4.) Later, in 2020, another modification was made to the software relating to scanner software (denominated 5.5-A GA) and approved on April 13, 2020 by EAC. Georgia conducted pilot elections in 2019 and some early voting during the March 2020 primary (before it was postponed and combined with the statewide primary) on the system while this certification was pending.

[23] Dr. Coomer previously served as Vice President of U.S. Engineering for Dominion and prior to that was the Vice President of Research and Development for Sequoia Voting Systems. He has worked in product development for election systems since 2005. He obtained his Masters degree and Ph.D. in nuclear physics and plasma physics from the University of California, Berkeley and a bachelor of science degree in engineering physics from Rensselaer Polytechnic Institute. (Tr. Vol. II at 99-100.) He additionally testified that he had designed the vote adjudication system used by Dominion, had written code for various election components, and provides primary election support for major Dominion customers.

[24] Additionally, witness declarations and testimony given in connection with earlier preliminary injunction motions was available for consideration to the extent that it was relevant and filed in the record.

[25] The Court's August 15, 2019 Order provided this explicit remedial relief: "The Secretary of State's Office should work with its consulting cybersecurity firm to conduct an in-depth review and formal assessment of 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." (Doc. 579 at 150.) The consulting firm referenced is Fortalice.

[26] Other cybersecurity experts such as Mr. Hursti also appear to have also consulted with Dr. Halderman in this process.

[27] The Defendants sought this confidentiality for two purposes: to protect the confidentiality and secrecy of this portion of the election system's functioning as well as to protect Dominion's confidential intellectual property pursuant to its contract with the State.

[28] Dr. Halderman is a Professor of Computer Science and Engineering and Director of the University of Michigan Center for Computer Security and Society. He is a nationally recognized expert in cybersecurity and computer science in the elections field. He testified before the United States Senate Select Committee hearings held on the topic of on Intelligence held on Russian interference in the 2016 U.S. Elections. His testimony and work was referenced in the Senate Committee's report. Professor Halderman has testified multiple times in this case.

[29] The Defendants disputed this evidence and implied the existence of other possible factors. Given that Dr. Halderman's testimony was presented under seal, the Court only describes this portion of the evidence in a general manner.

[30] As will be discussed further later in this Order, Dr. Stark serves on the Advisory Board of the U.S. Election Assistance Commission and as a member of the EAC's cybersecurity committee. (Doc. 296-6.) Dr. Appel is the

Eugene Higgs Professor of Computer Science at Princeton University and has over 40 years' experience in computer science and 15 years if experience in studying voting machines and elections. He has served as Editor in Chief of ACM Transactions on Programming Languages and Systems, the leading journal in his field. (Doc. 681-3). Dr. DeMillo is the Chair of Computer Science at Georgia Tech University. He previously served as the Director of the Georgia Tech Center for Information Security and Chief Technology Officer for Hewlett-Packard. (Doc. 548 at 74; Doc. 579 at 34.) Dr. DeMillo has conducted research 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 has also served on the advisory boards of Verified Voting and the Open Source Election Technology Institute. (*Id.*)

[31] The Court makes this point not as a criticism of Dr. Halderman but simply to point out that due to a variety of circumstances and the timing of the Court's ruling on the Defendants' motion to dismiss the BMD claims at a late date, discovery did not proceed here until the eleventh hour — and only then on a highly expedited, curtailed basis prior to the preliminary injunction motion.

[32] There was some back and forth in the parties' submissions regarding one of Dr. Halderman's affidavits pointing to a 2019 finding of one or more of the Texas Secretary of State's examiners' determining that Dominion's Democracy Suite 5.5-A version was substantively deficient and did not meet certification standards. Dr. Coomer dismissed the significance of that one report in his affidavit in this case. Ultimately, on January 24, 2020, the Texas Secretary of State's Office, based on the multiple reports of different Texas examiners on varied technical and substantive issues, concluded along lines quite close to Dr. Halderman's ultimate opinion in this case that certification should be denied. The Texas Secretary of State's Office found this same Dominion 5.5-A version should be denied certification for use in Texas elections on this basis: "The examiner reports identified multiple hardware and software issues that preclude the Office of the Texas Secretary of State from determining that the Democracy Suite 5.5-A system satisfies each of the voting-system requirements set forth in the Texas Election Code. Specifically, the examiner reports raise concerns about whether the Democracy Suite 5.5-A system is suitable for its intended purpose; operates efficiently and accurately; *and is safe from fraudulent or unauthorized manipulation.* Therefore, the Democracy Suite 5.5-A system and corresponding hardware devices do not meet the standards for certification prescribed by Section 122.001 of the Texas Election Code." https://www.sos.texas.gov/elections/laws/dominion.shtml (last visited September 25, 2020) (emphasis added). The Court also notes, though, that there are other jurisdictions that have approved the certification of the 5.5-A system, as Defendants assert. As noted in the affidavit of Jack Cobb, Defendant's witness who is the Laboratory Director for Pro V & V, the State of Pennsylvania has certified Dominion's Democracy Suite 5.5-A for usage. The Report of the Pennsylvania Commonwealth of Pennsylvania Department of State approving the usage of Democracy Suite 5.5. and 5.5A (in Pennsylvania jurisdictions choosing to utilize it), highlights that the approval is given "provided the voting system is implemented with the conditions listed in Section IV" of the Report. Commonwealth of Pennsylvania, Department of State, Report Concerning the Examination Results of Dominion Voting Systems Democracy Suite 5.5A With ImageCast X Ballot Marking Device (ICX-BMD), Image-Cast Precinct Optical Scanner (ICP), Image-Cast Central Station (ICC), and Democracy Suite EMS (EMS), *available at* https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/Dominion%20Democracy%20Suite%205.5-A/Dominion%20Democracy%20Suite%20Final%20Report%20scanned20with%20signature%20011819.pdf (emphasis in original.) These conditions are substantive, addressing items ranging from system security and prohibition of the connection of the system's components with any interface with modems or networks, to requirements for manual statistical audits, robust Logic and Accuracy testing on each device, voter education and warnings, needed voter instruction changes, and a host of other proactive substantive measures. Pennsylvania's review indicates that jurisdictions using the Dominion system do so in principal part with a *hand-marked ballot* based version of the system in tandem with scanners for vote tabulation. However, all voters are given the opportunity to use the ADA compliant marking device feature of the Democracy Suite 5.5 A. System.

[33] However, as Plaintiffs' experts Mr. Liu and Dr. Halderman testified in their respective affidavits in connection with the instant motions, BMDs use an Android operating system that is more than five years old and outdated.

[34] *See generally*, Mr. Liu testimony, Tr. Vol. II, Mr. Liu Declaration at Doc. 855-2; Dr. Halderman testimony, Tr. Vol II and Vol. III (and in conjunction with both preceding preliminary injunction hearings and related filings); Dr. Halderman Declarations at Docs. 785-2, 855-1; Mr. Skogland testimony, Tr. Vol. III; Mr. Skoglund Declarations at Docs. 853-5, 853-6; Dr. Appel Declaration, Doc. 855-3; Mr. Hursti testimony, Tr. Vol. I; Hursti Declarations at

Docs. 809-3, 800-2, 680-1; Dr. DeMillo Declarations, Docs. 285, 716-1; Dr. Stark testimony, Tr. Vol. I; Dr. Stark Declaration, Doc. 809-2.

[35] Pro V&V, Inc., a private company, is a National Institute of Standards Technology (NIST) Accredited Voting Systems Test Laboratory (VSTL) and a United States Election Assistance Commission Accredited Voting Systems Laboratory.

[36] Pro V&V similarly was previously retained by the Secretary of State and certified Georgia's DRE system in 2012 to the EAC. (Tr. Vol. II at 233.) The company's last October 2, 2020 report is addressed later in this Order. The EAC has as of the date of this Order not approved or acted upon this last recommendation.

[37] Mr. Cobb's second affidavit referenced the basis of his earlier statements regarding encryption as Dominion documentation about digital signing and encrypting. "My statement about digital signing and encrypting ... come directly from Dominion Voting 2.2 — Democracy Suite System Overview Version 5.5:146 Dated August 18, 2018 Section 2.6.1 Electronic Mobile Ballot" that describes QR barcode encoded data as encrypted." (Doc. 865-1.)

[38] Tr. Vol. II at 236.

[39] Pro V&V had conducted an assessment of an earlier version of the Dominion Democracy Suite software.

[40] Pro V&V's August 2019 certification documentation indicates that "[t]he state certification test was not intended to result in exhaustive tests of system hardware and software attributes." (*See* discussion of this in Dr. Halderman's affidavit, Doc. 785-2 at 10.)

[41] Mr. Liu further explained that his firm performs this consulting work for 8 of the top technology companies in the world, 10 of the top 20 retailers, 5 of the 10 top media companies. (Tr. Vol. II at 54; Liu Decl., Doc. 855-2.) At Honeywell, Dr. Liu led the penetration testing team for Honeywell International's global security team, "where our mission was to assess and breach the security of Honeywell's IT infrastructure and applications." (Doc. 855-2 at 2.)

[42] Mr. Liu indicated that the Android system in use was over half a decade out of date, with known vulnerabilities. (Tr. Vol. II at 68.) Similarly, Dr. Halderman noted that the Android OS versions used on the Dominion BMDs do not have the latest security features of later Android releases. (Halderman Decl., Doc. 785-2 at 9-11.)

[43] Dr. Halderman suggests that the "test mode" that the equipment was "on" when delivered was designed to limit his testing capacity. And on the other hand, Defendants imply in their questioning that Dr. Halderman may have modified the equipment in some other fashion. The Court sees no value in such guessing now.

[44] As discussed later, Mr. Hursti testified based on his cybersecurity experience and observations, that a host of the game and other applications on the servers and equipment he observed as well as internet connectivity created an obvious source for injection of malware.

[45] Mr. Liu's and Dr. Halderman's testimony and declarations, addressed earlier, discussed their views of the fallibility of this approach.

[46] The Court's Opinion and Order of September 28, 2020 (Doc. 918) addressed in depth issues relating to the PollPads and the continuation of prior issues involving the ENET database and program. The Court therefore does not revisit these issues here.

[47] Voting Machine Hacking Village 2019 Annual Report, pp. 17-18, media.defcon.org > voting-village-report-defcon27 (last visited October 8, 2020). (*See* Doc. 619-3.)

[48] "Hardening is the standard basic security practice under the well-accepted principle that a general-purpose device when used with a lot of software for different purposes is more vulnerable than a limited system which has

[includes only] the minimum necessary to accomplish the task." This is accomplished by "eliminating and removing all unnecessary services, and removing all drivers to make it the bare bone minimum needed for the task. And that is by reducing using the attack surface making it inherently more secure." (Hursti testimony, Tr. Vol. 1 at 126-27.) "In essence, hardening is the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle it is to the reduce the general purpose system into a single-function system which is more secure than a multipurpose one. Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, grant accounts and programs with the minimum level of privileges needed for the tasks and create separate accounts for privileged operations as needed, and the disabling or removal of unnecessary services." (Hursti Decl., Doc. 809-2 ¶ 28.) "Computers performing any sensitive and mission critical tasks such as elections should unquestionably be hardened. Voting system are designated by the Department of Homeland Security as part of the critical infrastructure and certainly fall into the category of devices which should be hardened as the most fundamental security measure." (*Id.* ¶ 29.) Hursti's personal first-hand observations and review of server log entries "confirmed that services which would have been disabled in the hardening process are running on the server." (Hursti Decl., Doc. 853-2 ¶ 6.) And he testified that it was visibly evident that "this system was not hardened both based on icons observed" and on "logs showing all programs running, all drivers running, and software installed. And that list is comprehensively proving that the system has been not hardened." (Tr. Vol. 1 at 127.)

[49] "The most basic security practice is never to let the operators have privileges to delete or alter log events, because that makes supervision impossible and performing forensics difficult, if not impossible. In addition, trustworthy logs are essential to detect and deter malicious software or intrusion." (Doc. 853-2 at 12.)

[50] Based on the sudden change in circumstances, the Court issued an express directive that the State Defendants file information and documentation as to the timing of the production of the testing documents to Pro V&V and the EAC. (*See* Doc. 957.)

[51] HAVA authorized the creation of the Election Assistance Commission as an independent, bipartisan organization, to establish minimum election administration and equipment standards in the administration of federal elections. (Issues with Florida's election machines in the 2000 presidential election were one of the triggers for Congress's creation of the Commission.) While state participation in EAC's review and approval regime is voluntary, once a state has elected to do so as in Georgia's case, the EAC treats state compliance with its standards and procedures as required. There is no provision for half compliance or half participation in EAC's review procedures. On the other hand, the EAC is not vested with actual coercive regulatory authority and thus relies on state cooperation in connection with compliance with its standards and determinations.

[52] Given the nature of the communications between counsel reflected in Plaintiffs' filing of October 6, 2002, the Court does not know what documents precisely were filed with the EAC.

[53] Both Dr. Halderman and Mr. Skoglund's affidavits discuss a host of problems that they have seen arise with last minute software fixes that are not thoroughly tested and evaluated for impact on the rest of the software system and in connection with use on a copy of the actual database. Dr. Halderman discusses the analogy — i.e., worst case scenario — of what happened with Boeing's late "minor" software fix in its Boeing 737 Max plane. Halderman and Skoglund's affidavits also discuss the security risks posed by last minute installation of software in voting machines in their experience.

[54] Ga. Comp. R. & Regs, 183-1-12-.08, new Rule adopted January 23, 2020, eff. Feb. 12, 2020; amended March 2, 2020 and eff. March 22, 2020.

[55] The county voting machines involved were not the ones now used in Georgia.

[56] State Defendants' counsel has pointed to two counties' successful flagging of the U.S. Senate ballot problem through their L & A testing. The Court agrees — this was a positive net result of the testing. For that very reason, though, thorough L & A testing, consistent with standard protocols across the country and Georgia law, would seem to be essential.

[57] Dr. Stark is a Professor of Statistics and Associate Dean of Mathematical and Physical Sciences at the University of California, Berkeley, a faculty member in the Graduate Program in Computational Data Science and Engineering, a co-investigator at the Berkeley Institute for Data Science, and was previously the Chair of the Department of Statistics and Director of the Statistical Computing Facility. (Decl. of Philip B. Stark, Doc. 296.) He has published hundreds of articles and books and has served on the editorial boards of academic journals in physical science, applied mathematics, computer science, and statistics and is a coauthor on a number of papers on end-to-end cryptographically verifiable voting systems, including being on the development team for the STAR-Vote system for Travis County, Texas. (*Id.*; Tr. Vol. I at 57.) Dr. Stark has consulted for many government agencies and currently serves on the Advisory Board of the U.S. Election Assistance Commission and its cybersecurity subcommittee. He also served on former California Secretary of State Debra Bowen's Post-Election Audit Standards Working Group in 2007. In addition to testifying as an expert in statistics in both federal and state courts, Dr. Stark has testified before the U.S. House of Representatives Subcommittee on the Census and the State of California Senate Committee on Elections, Reapportionment and Constitutional Amendments, and before California Little Hoover Commission about election integrity, voting equipment, and election audits. Dr. Stark's statistical "risk-limiting audits" approach to auditing elections has been incorporated into statutes in several states including California, Colorado, Rhode Island, and in some respects in Georgia's new Election Code. (Doc. 296; Doc. 640-1; Tr. Vol. I at 83.) Dr. Stark pioneered the introduction of RLAs in state sponsored studies and elections in California and Colorado. (Stark Decl., Doc. 296; Stark Suppl. Decl., Doc. 680-1 ¶ 17.)

[58] Smaller risk limits require stronger evidence that the outcome is correct: All else equal, the audit examines more ballots if the risk limit is 1% than if it is 10%. Lindeman and Stark (2012) at 1. Similarly, smaller (percentage) margins require more evidence, because there is less room for error. *Id.*

[59] RLAs therefore "address limitations and vulnerabilities of voting technology, including the accuracy of algorithms used to infer voter intent, configuration and programming errors, and malicious subversion." Lindeman and Stark (2012) at 1. This is one reason why the NAS has endorsed the use of risk-limiting audits of human-readable, voter-verifiable paper ballots. NAS Report at 94-95.

[60] Dr. Stark's auditing principles are in line with the recommendation of the NAS:

An evidence-based election would produce not only a reported (or initial) election outcome, but also evidence that the reported outcome is correct. This evidence may be examined in a "recount" or in a "postelection audit" to provide assurance that the reported outcome indeed is the result of a correct tabulation of cast ballots.

Voter-verifiable paper ballots provide a simple form of such evidence provided that many voters have verified their ballots. The ability of each voter to verify that a paper ballot correctly records his or her choices, before the ballot is cast, means that the collection of cast paper ballots forms a body of evidence that is not subject to manipulation by faulty hardware or software. These cast paper ballots may be recounted after the election or may be selectively examined by hand in a post-election audit. Such an evidence trail is generally preferred over electronic evidence like electronic cast-vote records or ballot images. Electronic evidence can be altered by compromised or faulty hardware or software. Paper ballots are designed to provide a human-readable recording of a voter's choices. The term "paper ballot" here refers to a "voter-verifiable paper ballot," in the sense that voters have the opportunity to verify that their choices are correctly recorded before they cast their paper ballots. The voter may mark the ballot by hand, or the marked ballot may be produced by a voting machine. In the current context, the human-readable portion of the paper ballot is the official ballot of record that acts as the record of the voter's expressed choices. Rather than, for example, an electronic interpretation of the paper ballot or a non-human readable barcode appearing on a ballot.

(NAS Report at 94-95.)

[61] Dr. Gilbert also was a member of the National Academies of Science, Engineering and Medicine Committee on the Future of Accessible Voting: Accessible Reliable, Verifiable Technology, among other leadership and publishing accomplishments. (*See* Doc. 658-2.) Dr. Gilbert's research currently focuses on human use of technology and access to voting systems rather than cybersecurity or cyber engineering issues. His testimony focused on the comparative benefits of the BMD system, its broad human accessibility, its automated generation of a paper ballot

that voters have the opportunity to review, and how and if the system's use of a QR code impacts its auditability. Dr. Gilbert's background and expertise is not in the field of statistics.

[62] Dr. Halderman and Matthew Bernhard co-authored their research in a May 2020 published article, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" A number of the experts referenced the paper, which discusses low rates of voter verification of ballots and the degree to which that may be increased by different voter prompts It also constitutes part of the research literature that bears on the issues of the validity of RLAs where BMDs are used that tabulate the vote based on a QR code rather than the readable information that voters might review.

[63] VotingWorks is a vendor of barcoded ballot-marking devices just like the Dominion system. (Tr. Vol. II at 281.)

[64] In response to the Court's question about the methodology of the Arlo software which incorporates Dr. Stark's statistical algorithm, Dr. Adida admitted, "I'm going to tell you my best understanding of it and admit that there is a level of statistics that goes a little bit outside of my expertise ... And exactly how that is done, that is where my expertise stops and Dr. Stark's begins." (Tr. Vol. II at 302-303.)

[65] Most of the states where VotingWorks has assisted in conducting RLAs primarily use hand-marked paper ballots with BMDs used only for voters with accessibility needs. These include Virginia, Michigan, Missouri, and Rhode Island. In California, and Pennsylvania, the majority of the voters in the state use hand-marked paper ballots and only certain jurisdictions in those States use BMDs for all voters. In Ohio, there is no uniform voting system; instead roughly half of the jurisdictions use hand-marked paper ballots, a handful use DREs with voter verified paper audit trails, and a handful use BMDs. *See* Verified Voting, The Verifier, *available at* https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020.

[66] Other criticisms raised focused on the statistical invalidity of auditing only one race and the absence of any meaningful audit trail.

[67] According to the NAS Report:

RLAs can establish high confidence in the accuracy of election results—even if the equipment that produced the original tallies is faulty. This confidence depends on two conditions: (1) that election administrators follow appropriate procedures to maintain the chain-of-custody and secure physical ballots—from the time ballots are received, either in-person or by mail, until auditing is complete; and (2) that the personnel conducting the audit are following appropriate auditing procedures and the equipment and software used to audit the election are independent of the equipment and software used to produce the initial tallies. In the latter case, this not only requires that the software be independent of the software used to tally votes, but also that the software's specifications/algorithms, inputs, and outputs are transparent to permit members of the public to reproduce the software's operation.

(NAS Report at 96.) As Dr. Stark has attested, the BMDs are not software independent and therefore cannot establish high confidence in the accuracy of the results "even if the equipment that produced the original tallies is faulty."

[68] There are two general types of risk-limiting audits: ballot-polling audits and comparison audits (either ballot-level comparison or batch comparison). Lindeman and Stark (2012) at 2, 6. Ballot-polling audits are a bit like exit polls, but instead of asking randomly selected voters how they voted, they manually inspect randomly selected cast ballots to see the votes they contain. (Doc. 680-1 ¶ 18.) They require knowing who reportedly won, but no other data from the tabulation system. Lindeman and Stark (2012) at 2. Ballot-polling audits are the best method "when the vote tabulation system cannot export vote counts for individual ballots or clusters of ballots or when it is impractical to retrieve the ballots that correspond to such counts," i.e., systems like Georgia's that use precinct level tabulators that apply randomization to scanned ballots to protect voter anonymity. *See id.* In a ballot-polling RLA, "if a large enough random sample of ballots shows a large enough majority for the reported winner(s), that is strong statistical evidence that the reported winner(s) really won. It would be very unlikely to get a large majority for the reported

winner(s) in a large random sample of ballots if the true outcome were a tie, or if some other candidate(s) had won. There is deep mathematics behind proving out how large is "large enough" to control the risk to a pre-specified level, such as five percent. However, the calculations that determine when the audit can stop examining more ballots are relatively simple." (Doc. 680-1 ¶ 18.)

[69] Somewhat confusingly, Dr. Stark also testified that "[t]he sense in which a risk-limiting audit may still be worth doing is that it can catch — it can detect whether errors in the tabulation of a particular pile of ballots was large enough to alter the reported outcome of one or more contests. But what it can't do is determine whether that particular pile of paper is a trustworthy representation of what voters did, saw, or heard." (*Id.* at 68-69.) In other words, "[a]pplying risk-limiting audit (RLA) procedures to securely curated BMD printouts can check the accuracy of the tabulation of the printouts. It can provide confidence that if errors in scanning and tabulation were large enough to change the reported winner(s), that fact would be detected and corrected. But such an audit does nothing to check whether the BMDs printed incorrect votes, omitted votes, or printed extra votes. Risk-limiting audit procedures check the *tabulation of BMD printouts*; they do not check the *functioning of the BMDs*. They cannot confirm the outcome of elections conducted using BMDs." (Doc. 680-1 ¶¶ 6-7.) Similarly, he remarked that "[r]igorous audits can ensure (statistically) that tabulation errors did not alter the reported outcomes. But they cannot ensure that errors in BMD printouts did not alter the reported outcomes." (*Id.* ¶ 12.) While there appears to be some disconnect between the use of RLAs to check tabulations, it is possible Dr. Stark is referring to ballot-level or batch comparison RLAs here which, unlike ballot-polling audits, check outcomes by comparing a manual interpretation of ballots selected at random to the voting system's interpretation of those ballots counts.

[70] In conjunction with Dr. Adida's organization, VotingWorks, the State of Georgia consulted with the Verified Voting Foundation when it conducted a RLA pilot of two election contests in Cartersville in November 2019. (680-1 ¶ 17.) Dr. Stark was on the Board of Directors of Verified Voting for years until he resigned after the President of Verified Voting declined to clarify publicly that the Cartersville pilot audit did not "confirm outcomes" or show that the voting system worked correctly. (*Id.* ¶ 23.) Since that time, Verified Voting's official positions on RLAs and BMDs have for the most part realigned with Dr. Stark's findings and opinions. (Tr. Vol. I at 80.) *See* Statement on Ballot Marking Devices and Risk-Limiting Audits, *available at* https://verifiedvoting.org/statement-on-ballot-marking-devices-and-risk-limiting-audits/.

[71] Again, Dr. Stark invented virtually every extant method for performing risk limiting audits, including ballot-polling risk-limiting audits. Dr. Stark was the first person to pilot a ballot-polling risk-limiting audit, in Monterey, CA, in May, 2011. Dr. Stark published the first software tool to conduct ballot-polling risk-limiting audits which was the official tool used by the State of Colorado for its ballot-polling risk-limiting audits and is referenced in Colorado election regulations. (Doc. 809-2 ¶ 10.) The VotingWorks Arlo software to be used in Georgia's audit incorporates Dr. Stark's algorithm, and Stark understands that VotingWorks benchmarked the Arlo software against his to confirm Arlo is a correct implementation of the algorithm. (*Id.* ¶ 11.) Understandably, Dr. Stark strenuously disagrees with any attempts to redefine the RLA methodology so that it only corrects some kinds of errors or to modify its application for use on systems with an untrustworthy paper trail because such measures go against the whole principle the RLA was designed to fulfill and weakens the concept to a degree that it destroys the fundamental property that the audit has a large chance of correcting the election outcome if it is wrong. (Tr. Vol. I at 80-83.)

[72] In addition to a burden on the fundamental right to vote, Plaintiffs also assert in-person voters are subject to unequal treatment as compared to provisional and absentee voters whose paper ballots are capable of being meaningfully recounted, reviewed against an independent record to verify the accuracy of the vote tabulation, and may have discrepancies detected and corrected through audits.

[73] O.C.G.A. § 21-2-300(a)(2) (effective April 2, 2019) (mandating a new uniform statewide voting system that provides for "the use of scanning ballots marked by electronic ballot markers and tabulated by using ballot scanners for voting at the polls and for absentee ballots cast in person").

[74] Georgia law permits a registered voter to vote via absentee ballot for any reason. *See* O.C.G.A. § 21-2-380. Voters under age 65 must submit separate, distinct applications for each election (i.e. primary, general, runoff) sufficiently early to their county registrar's office to ensure timely receipt of their absentee ballot. O.C.G.A. § 21-2-

381(a)(1)(A); O.C.G.A. § 21-2-381(a)(1)(G). Absentee ballot applications may be denied if the registrar determines that the information provided by the voter in the application does not match the voter's information on file with the registrar's office or if the voter's signature on the absentee ballot envelope does not match the signature on their voter registration card. O.C.G.A. § 21-2-381(b)(2)(3). Once received and completed, voters must sign an oath on their absentee ballot envelope and personally mail or deliver their ballot to the board of registrars or absentee ballot clerk or to a dropbox. O.C.G.A. § 21-2-385(a). Georgia does not provide pre-paid postage for the return of the absentee ballot, and thus, voters must pay for their own return postage to vote by mail. The State of Georgia does not count mail ballots received after the closing of polls at 7:00 p.m. on Election Day. *See* O.C.G.A. § 21-2-386(a)(1)(F). This is true even if a ballot arrives late for reasons objectively outside the voter's control, and even if the ballot was postmarked weeks before Election Day or alternatively, on Election Day. Absentee ballots will be rejected if not received by election day or "[i]f the elector has failed to sign the oath, or if the signature does not appear to be valid, or if the elector has failed to furnish required information or information so furnished does not conform with that on file ... or if the elector is otherwise found disqualified to vote[.]" O.C.G.A. § 21-2-386(a)(1)(C).

[75] The first initial motions for preliminary injunction seeking to enjoin the BMD system, filed in October 2019 (Docs. 619, 640), were denied without prejudice in August 2020. At that juncture, the Court viewed the evidence as presented as closer to a quasi-facial challenge rather than one that was rooted, at least in part, in the record evidence involving the actual use of the BMD machines and associated Dominion equipment and attached KnowInk registration check-in PollPad tablets at voting precincts. Covid-19 pandemic ramifications triggered major election scheduling delays and changes that resulted in the March presidential primary being moved ultimately to early June 2020.

[76] *See* Court's Opinion and Order of September 28, 2002. (Doc. 918.)

[77] Sections (b) and (c) of O.C.G.A. § 21-2-438 provide as follows:

(b) At elections, any ballot marked by any other mark than a cross (X) or check (✓) mark in the spaces provided for that purpose shall be void and not counted; provided, however, that no vote recorded thereon shall be declared void because a cross (X) or check (✓) mark thereon is irregular in form. A cross (X) or check (✓) mark in the square opposite the names of the nominees of a political party or body for the offices of President and Vice President shall be counted as a vote for every candidate of that party or body for the offices of presidential elector.

(c) Notwithstanding any other provisions of this chapter to the contrary and in accordance with the rules and regulations of the State Election Board promulgated pursuant to paragraph (7) of Code Section 21-2-31, if the elector has marked his or her ballot in such a manner that he or she has indicated clearly and without question the candidate for whom he or she desires to cast his or her vote, his or her ballot shall be counted and such candidate shall receive his or her vote, notwithstanding the fact that the elector in indicating his or her choice may have marked his or her ballot in a manner other than as prescribed by this chapter.

[78] According to the Dominion contract, for each ballot scanned, a corresponding ballot image is created and stored for audit purposes, that consists of two parts: (1) the scanned image of the ballot; and (2) machine generated text showing each mark that the scanner interpreted for that particular ballot, referred to as the AuditMark. (Doc. 619-8 at 57.)

[79] A potential explanation for the phenomenon of some voters marking their absentee ballots without filling in the designated oval is two-fold. Hand marked ballots, where votes were cast with an X or check, were used prior to the introduction of the DRE system in Georgia in 2002. And this may be found in Georgia's existing election regulation that contains different provisions for vote tabulation in statewide versus municipal elections. *See* Rule 183-1-15-.02(2)(2)&(3). The Dominion BMD/optical scan system is required to be used in all statewide elections. But Georgia still allows for other voting systems to be used in non-statewide "municipal" elections (*see* provisions of rule that still pertain to lever systems, Rule 183-1-15-.02(2)(1) and non-optical scan, i.e., hand counted paper ballots, Rule 183-1-15-.02(2)(3)). For optical scan paper ballots, the voter must "fill in the oval" to mark their vote choice. Rule 183-1-15-.02(2)(2)(a). But for non-optical scan paper ballots, the voter must "place an X, a check, or other similar

mark" in a square to mark their vote choice. Rule 183-1-15-.02(2)(3)(a). This might account for why a number of voters are placing either an X or a check in the oval rather than filling it in and may create a problem if the ICP and ICC scanners in operation disregard these types of markings on the optical scan ballots without further review. Further, the Court notes, that prior to the instant 2020 ballot cycle, a vote with an X or check on an absentee or provisional ballot would not have been subject to adjudication software review programmed to kick out marks that were too light to register on the scanner, but to the human eye were visible as an X or check vote designation.

[80] The ImageCast Precinct Scanner and Tabulator is an optical scan ballot tabulator used to scan marked paper ballots and interpret voter marks on the paper ballot. It is a proprietary Dominion product. (Tr. Vol. II at 81.)

[81] The ImageCast Central Scanner consists of a Canon DR-G1130 commercial off-the-shelf digital high-speed document scanner configured to work with the ImageCast Central Software for high speed ballot tabulation.

[82] The scanner does not work like a camera — it does not take a picture of the paper ballot. (Tr. Vol. I at 140-41.)

[83] According to Dr. Coomer, when an in-person voter scans a hand-marked paper ballot (i.e., an emergency ballot) on the precinct scanner, the scanner will alert the voter if the ballot is rejected as having contained an ambiguous mark and that voter will have the opportunity to correct the ballot. (Tr. Vol. II at 75-76; *see also* Ex. M to Hursti Decl., Doc. 809-3 at 48.) However, because of the configuration of the ICP scanner in Georgia, if the voter marked a selection, but the scanner did not recognize that as a vote, the voter would not be alerted if an undervote is detected for a particular contest. (Tr. Vol. II at 75.) The ICP will only alert an in-person voter if the ballot is completely blank for all races. (*Id.* at 76.)

[84] As shown in Exhibit 7.1, the ballot image on the left illustrates what the ballot looks like to the human eye when voted. The ballot image on the right shows the ballot recorded by the ICP scanner and is the image that is tabulated for vote counting.

[85] To be fair to his testimony, Mr. Hursti opined that in order to maximize the accuracy of the ICC tabulation scanner, the ICC should be configured to capture additional information from the images, such as gray scale or color, in addition to an increase in the DPI.

[86] This is consistent with the representations made in the Dominion contract that "[a]fter a ballot is adjudicated, the ballot image is appended with a record of that decision including the user's name, action taken by the user, and date and time of the action. This adjudication AuditMark is appended to the ballot image under the original AuditMark, which was manifested during tabulation." (Doc. 619-8 at 54.)

[87] An overvote occurs when the scanner/tabulator registers more than one legible vote for a single contest.

[88] This is the result unless they can be discovered in a subsequent manual recount, like the one conducted by Clarke County that recovered some of these types of lost votes by allowing full examination of the ballots with "blanks" in the 5 districts where such recounting was allowed. The panel's bipartisan members agreed on all of the vote determinations.

[89] *See* *Elrod v. Burns*, 427 U.S. 347, 373, 96 S.Ct. 2673, 49 L.Ed.2d 547 (1976) (plurality opinion) (The "loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury."); *Martin v. Kemp*, 341 F. Supp. 3d 1326, 1340 (N.D. Ga. 2018) ("The Court finds that [p]laintiffs have established irreparable injury as a violation of the right to vote cannot be undone through monetary relief and, once the election results are tallied, the rejected electors will have been disenfranchised without a future opportunity to cast their votes."); *see also* *League of Women Voters of N.C.*, 769 F.3d at 247 ("Courts routinely deem restrictions on fundamental voting rights irreparable injury ... [because] once the election occurs, there can be no do-over and no redress. The injury to these voters is real and completely irreparable if nothing is done to enjoin the law.").

[90] Although the burden is minimal, the evidence indicates the instructions are not effective or are ignored by a number of voters.

[91] This deadline can be extended by the Secretary of State, if necessary, in order to perform an audit.

[92] On the other hand, during his September 10th testimony before this Court, Mr. Hursti seemed to indicate that no other system configuration adjustments could be made to increase the accuracy of the ICP tabulators used at precinct locations. Instead, his proposed solution for the ICP precinct scanner is to provide better instructions to voters carefully to fill the whole oval and provide all voters with black felt ink pens for marking paper ballots by hand. (Tr. Vol. I at 141, 159, 168.) According to Mr. Hursti, the evidence demonstrates that many voters do not follow the existing written instructions printed on the absentee/provisional/emergency paper ballots — an indication that the instructions have not been effective. (*Id.* at 159.) The CES study similarly concluded that instructions to voters should be modified to inform the voter to fill in the oval next to the candidate name and to avoid circling, underlining, or placing checkmarks or Xs, or otherwise marking the candidate name outside the vote target oval. The CES study also determined that voters should be warned to not use red ink when marking ballots. The Court takes judicial notice that the Secretary of State has revised the written instructions on its paper ballots to incorporate these recommendations from the CES study, though its revised ballot instructions removed the visual illustration showing how to blacken in the oval. And the Secretary of State's guidance on the use of emergency paper ballots for in-person voting specifies that precincts provide only the two pens approved by Dominion Voting — the Sharpie Fine Point black pen and the Paper Mate Flair M Medium Point black pen.92 (*See* Pls.' Ex. 11.) The casting of hand marked emergency ballots in prior elections in the 2020 election cycle appears to have been fairly rare based on the evidence before the Court. However, as the Secretary of State's Office and County Registrar's Offices should be providing more training to county poll workers on the State's emergency ballot options and process prior to the 2020 general election, a focus upon scanning issues impacting the scanning of hand marked ballots at the precinct level, where scanners produce even less refined images, would be sensible.

[93] The Court recognizes that some counties have indicated they do not plan to use the adjudication software and will proceed according to their established procedures to systematically review scanned hand marked ballots along with the original ballots, consistent with the penultimate "voter intent" standard established under Georgia law.

[94] Dr. Coomer, however, testified that the scanner software (not the adjudication software) is programmed to provide an alert where a ballot is scanned that registers as completely blank.

[95] Every hand-marked paper ballot has a unique corresponding ballot ID number printed at the bottom that is recorded by the scanner/tabulator and reflected on the AuditMark associated with the ballot image. The AuditMark that indicates the disposition of the candidate choices on each scanned ballot contains a record of the ballot ID from the paper ballot. The AuditMark on the scanned ballot image is therefore traceable to the original paper ballot. As a result, the original paper ballots can be compared, as needed under the circumstances, to the AuditMark to confirm that voter intent has been accurately recorded by the scanners.

[96] To the extent questions arise whether voter marks are clearly discernible on the scanned image, the Vote Review Panels can review the original paper ballots if necessary. Every hand-marked paper ballot has a unique corresponding ballot ID number printed at the bottom that is recorded by the scanner/tabulator and reflected on the AuditMark associated with the ballot image. The AuditMark that indicates the disposition of the candidate choices on each scanned ballot contains a record of the ballot ID from the paper ballot. The AuditMark on the scanned ballot image is therefore traceable to the original paper ballot. As a result, the original paper ballots can be compared, as needed under the circumstances, to the AuditMark to confirm that voter intent has been accurately recorded by the scanners.

[97] *See, e.g.*, Paragraph (a) of proposed Order at Doc. 809-17.

[98] Justice Ruth Bader Ginsburg — Opening Remarks to Senate Judiciary Committee in her 1993 Senate Confirmation Hearing.

[99] For the reasons discussed in Section III D, the Coalition Plaintiffs' Motion is GRANTED IN PART in connection with the scanner/tabulator settings in tandem with Dominion's adjudication software that as currently configured allow certain voter marks on hand-marked absentee and provisional ballots to disregarded and not be counted.