IN THE UNITED STATES DISTRICT COURT
FOR THE NOTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, et al.,	)	
	)	
Plaintiffs,	)	**Civil Action No.**
	)	**1:17-cv-02989-AT**
v.	)	
	)	
BRIAN KEMP, et al.,	)	
	)	
Defendants.	)	

***AMICUS CURIAE* BRIEF IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS AND IN SUPPORT OF PLAINTIFFS' ANTICIPATED REQUEST FOR PRELIMINARY INJUNCTION BY *AMICI CURIAE* COMMON CAUSE, NATIONAL ELECTION DEFENSE COALITION, AND PROTECT DEMOCRACY**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Additional Authorities

INTRODUCTION

This litigation raises issues of vital importance to Georgia and the Nation. Defendants' motion to dismiss the Coalition Plaintiffs' Third Amended Complaint ("TAC") relies on the assertion that Plaintiffs allege only "purely speculative injuries." Dkt. 234-1 at 10-11. To the contrary, overwhelming evidence in the public record establishes that the threat to all Plaintiffs' constitutional rights posed by the use of *unreliable* and *unverifiable* voting machines in the upcoming November election is very real. Without relief from this Court, Plaintiffs face an imminent, serious threat that Defendants' use of the paperless Diebold AccuVote TS/TSx system, a direct recording electronic voting system with no voter-verified paper audit record ("paperless DRE"), coupled with Defendants' failure to properly safeguard Georgia's voting system, will result in undetectable and irreversible miscounting or dilution of their votes in the November 2018 election.

Plaintiffs' legal claims reflect a growing consensus about the elements of a voting system that are essential to safeguard against cyberattacks and uncorrectable errors. Director of Homeland Security Kirstjen Nielsen recently testified to the U.S. Senate that "[n]ot having a verifiable way to audit election results in some states [like Georgia] represents a '*national security concern*.'" Volz & Zengerle, "Inability to audit U.S. elections a 'national security concern': Homeland chief,"

Reuters (March 21, 2018) (emphasis added). Secretary Nielsen was unequivocal: "You *must* have a way to audit and verify the election result."[1] Despite a chorus of similar warnings from national security and technology experts from across the political spectrum, Defendants continue to maintain an electronic voting system that provides *no* verifiable way to audit election results to determine if any error affected those results, including errors resulting from malicious tampering, inadvertent software bugs, or mistakes in administration. The substantial risk that use of this unreliable and unverifiable system in the upcoming election will result in unconstitutional miscounting or dilution of Plaintiffs' votes not only establishes Plaintiffs' standing, but also justifies preliminary injunctive relief.

A. Plaintiffs face a "substantial risk" of irreparable harm

Plaintiffs do not need to allege that a breach or error in Georgia's vulnerable election system is absolutely certain to occur, or even is more likely than not, in order to seek relief from this Court. "An allegation of future injury" is enough to establish standing if "there is a ' "substantial risk" that the harm will occur.' " *Susan B. Anthony List v. Driehaus*, 134 S.Ct. 2334, 2341 (2014) (quoting *Amnesty International USA v. Clapper*, 568 U.S. 398, 414 n.5 (2013)); *see Spokeo v.*

[1] *See* https://www.youtube.com/watch?v=lXjYNLJ9yAM&feature=youtu.be (video of testimony at 3:38; emphasis added).

Robins, 136 S.Ct. 1540, 1549 (2016) ("risk of real harm" enough for standing).[2]

This bedrock principle has special force in the context of pending elections. "Justiciability in such cases depends not so much on the fact of past injury but on the prospect of its occurrence in an impending or future election." *Babbitt v. United Farm Workers National Union*, 442 U.S. 289, 300 n.12 (1979). Here, Plaintiffs "have standing based on an increased risk that their votes will be improperly discounted." *Stewart v. Blackwell*, 444 F.3d 843, 854 (6th Cir. 2006), *vacated and dismissed as moot before en banc rev.*, 473 F.3d 692 (6th Cir. 2007).

The actual risks that Plaintiffs' votes will be incorrectly recorded or diluted by incorrect counting of other votes makes this case fundamentally different from previous cases on which Defendants rely in which courts rejected challenges to

[2] *See also Arcia v. Fla. Sec. of State*, 772 F.3d 1335, 1341 (11th Cir. 2014); ("realistic probability" of harm); *Fla. State Conf. of the NAACP v. Browning*, 522 F.3d 1153, 1161 (11th Cir. 2008) ("'realistic danger'" of injury) (quoting *Babbitt v. United Farm Workers National Union*, 442 U.S. 289, 298 (1979)); *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 141, 153-55 (2010) ("substantial risk" that plaintiffs' alfalfa crops would be infected, and measures they took to avoid that risk, established standing "even if their crops are not actually infected"); *Friends of the Earth, Inc. v. Laidlaw Environmental Servs.*, 582 U.S. 167, 182-84 (2000) (plaintiffs' actions taken based on their "reasonable concerns" about effects of defendants' discharges established standing); *Bryant v. Yellen*, 447 U.S. 352, 367 (1980) (farmworkers had standing based on likelihood that land would become available at less than market prices, and thus that they *might* be able to purchase it).

paperless DREs.[3] The facts have fundamentally changed since the 2016 election. Risks that may have seemed hypothetical in the past are now very real. And there can be no question that the miscounting or diluting of Plaintiffs' votes – resulting from cyberattacks, software bugs, or other errors – will constitute grave irreparable harm. *See, e.g.*, *Ne. Ohio Coal. for Homeless v. Husted*, 696 F.3d 580, 599 (6th Cir. 2012) (failure to count ballot is irreparable harm). Defendants' motion to dismiss should be rejected, and the Court should promptly consider and grant Plaintiffs' anticipated motion(s) for preliminary injunctive relief.

B. Georgia's voting system is unacceptably vulnerable to manipulation

Among the many vulnerabilities of the election system Plaintiffs challenge, there is an essential defect: It relies on the Diebold AccuVote paperless DRE system to record votes. The federal officials tasked with the responsibility to protect our national security agree that paperless DREs "are at highest risk for security flaws," and "[s]tates should rapidly replace outdated and vulnerable voting

[3] *See Weber v. Shelley*, 347 F.3d 1101, 1103 (9th Cir. 2003) (plaintiff "raised at most a hypothetical concern"); *Wexler v. Anderson*, 452 F.3d 1226, 1232-33 (11th Cir. 2006) (challenging only differing recount procedures of "residual" ballots); *Favorito v. Handel*, 285 Ga. 795, 797-99 (2009) (following *Weber* and *Wexler*); *Banfield v. Cortes*, 631 Pa. 229, 266 (2015) (rejecting state law claims where plaintiffs "presented no evidence to suggest that DREs are any less accurate than any other voting system"); *Andrade v. NAACP of Austin*, 345 S.W.3d 1, 15 (Tex. 2011) (similar); *Stein v. Cortes*, 223 F.Supp.3d 423, 427, 432 (E.D. Pa. 2016) (post-election challenge; plaintiff did not even *allege* recount might change result).

systems" with machines that "[a]t a minimum … have a voter-verified paper trail …." Senate Select Comm. on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election* 4, 6 (May 8, 2018) ("SSCI Report").

Beyond the inherent vulnerability of all paperless DRE systems, numerous studies have found that the very system used in Georgia – the Diebold AccuVote TS/TSx system – and similar systems produced by the same manufacturer, contain specific security flaws that sophisticated hackers could readily exploit. In 2007, following a comprehensive, top-to-bottom review, California's Secretary of State decertified the Premier (formerly Diebold) AccuVote DRE systems because:

- Those systems "were inadequate to ensure accuracy and integrity of the election results and of the systems that provide those results";
- The systems "contain serious design flaws that have led directly to specific vulnerabilities, which attackers could exploit to affect election outcomes";
- "[T]he Diebold software contains vulnerabilities that could allow an attacker to install malicious software on voting machines and on the election management system, which could cause votes to be recorded incorrectly or to be miscounted, possibly altering election results";
- "[T]he Diebold system is susceptible to computer viruses that propagate from voting machine to voting machine and even voting machines to the election management system, which could allow an attacker with access to only one voting unit or memory card to spread malicious code, between elections, to many, if not all, of a county's voting units"; and
- "[D]ue to these shortcomings some threats would be difficult, if not impossible, to remedy with election procedures," including because attacks "could be carried out in a manner that is *not subject to detection by audit*,

including review of software logs."

California Secretary of State, *Withdrawal of Approval* 2, 3 (Oct. 25, 2007 Revision) (emphasis added). The Diebold systems found severely inadequate in that top-to-bottom review were newer – and thus presumably *more* secure – than Diebold machines currently in use in Georgia. *See* TAC ¶¶59, 82.

Ohio's Secretary of State commissioned a separate analysis that reached similar conclusions, including that flaws in Premier's (formerly Diebold's) election system "lead to a broad spectrum of issues that undermine the voting system's security and reliability," and "[t]he resulting vulnerabilities are exploitable by an attacker, often easily so, under election conditions." McDaniel, et al., *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing* 103 (Dec. 7, 2007).[4] Yet another official assessment, commissioned by the State of Maryland in 2003, identified "several high-risk vulnerabilities" in the Diebold AccuVote-TS system, and concluded that "[i]f these vulnerabilities are exploited, significant impact could occur on the accuracy, integrity, and availability of election results," and that "[t]he system … is at high risk of compromise." Science

[4] "Numerous vulnerabilities allow an attacker to modify or replace ballot definitions, to change, miscount, or discard completed votes, or to corrupt the tally processes." *Id.* The system is vulnerable to attacks that are "invisible after the fact," and the software is "unstable," causing "frequent crashes, system lock-ups, and unexplained errors." *Id.* at 103-04.

Apps. Internat'l Corp. (SAIC), *Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes* ii, v (Sept. 2, 2003).

Scholarly analyses have reinforced these findings, consistently exposing the substantial increased risks of vote tampering and miscounting created by use of Diebold's AccuVote DREs. As just one example, scholars at Princeton's Center for Information Technology Policy who analyzed a Diebold AccuVote-TS machine found it "is vulnerable to extremely serious attacks." Feldman, et al., "Security Analysis of the Diebold AccuVote-TS Voting Machine," *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop*, 1 (Aug. 2007).

> For example, an attacker who gets physical access to a machine or its removable memory card for as little as one minute could install malicious code; malicious code on a machine could *steal votes undetectably*, modifying all records, logs, and counters to be consistent with the fraudulent vote count it creates. An attacker could also create malicious code that *spreads automatically* and silently from machine to machine during normal election activities—a voting-machine virus. We have constructed working demonstrations of these attacks in our lab.

Id. (emphases added). Other scholarship has produced similarly stark results.[5]

[5] *See, e.g.*, Gardner, et al., "Software Review and Security Analysis of the Diebold Voting Machine Software." Security and Assurance in Information Technology (SAIT) Lab, Florida State University, 6, 30-35 (July 27, 2007) (listing 126 flaws in Diebold voting systems); Schwartz, "Computer Voting Is Open to Easy Fraud, Experts Say," *New York Times* (July 24, 2003) (Diebold election system used in Georgia "contains serious flaws that would allow voters to cast extra votes and permit poll workers to alter ballots without being detected") (discussing Kohno, et al., "Analysis of an electronic voting system," *Proceedings - IEEE Symposium on*

At a recent DEFCON conference, hackers with access to only legally and publicly available information were able to breach a range of actual voting machines. Blaze, et al., *DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure* 4, 8 (Sept. 2017). They noted that many of these machines include hardware components manufactured outside of the United States, which exposes voting machines to compromise "at the earliest of stages in [the] manufacturing process. For example, foreign actors could design or plant a virus in software, memory, or even a small microchip that could affect an entire make/model of voting machine, theoretically allowing them to be compromised in one coordinated attack." *Id.* at 15. Given the vulnerability of paperless DREs, the Senate Select Committee on Intelligence has concluded that vendors of DRE voting machines "represent an enticing target [f]or malicious cyber actors," and has highlighted the troubling reality that state authorities "have very little insight into the cyber security practices of many of these vendors." SSCI Report at 4.

The risks created by paperless DREs are not limited to in-person attacks, despite claims by vendors and some state officials that paperless voting machines

---

Security and Privacy, 27-40 (2004); Jones & Simons, *Broken Ballots: Will Your Vote Count?* 164-82, 205-06 (2012) (discussing numerous studies finding serious vulnerabilities in Diebold machines and systems).

are safe because they are never connected to the internet.

> [M]any polling places around the country transmit voting results to their county election offices via modems embedded in or connected to their voting machines.… Because of this, attackers could theoretically intercept unofficial results as they're transmitted on election night — or, worse, use the modem connections to reach back into election machines at either end and install malware or alter election software and official results.

Zetter, "The Myth of the Hacker-Proof Voting Machine," *New York Times Magazine* (Feb. 21, 2018); *see* Feldman, et al. at 5 (Diebold AccuVote-TS has slot "optionally containing a modem card used to transfer ballot definitions and election results"). And remote hacking is possible even without use of the modems. One scholar recently demonstrated his ability to steal votes by hacking the "same electronic voting machine used in Georgia" and posting a video online explaining how attackers could infect these machines by emailing a virus to election officials responsible for programming the machines with the ballot definition files for each election. Halderman, "I Hacked an Election. So Can the Russians," *New York Times* (April 5, 2018) (video at 1:18, 1:49-2:30).

Indeed, the House Permanent Select Committee on Intelligence recently concluded that even if "voting machines themselves, as well as tabulation systems, are not directly connected to the internet [that] does not offer adequate security. Rather, it can create a false sense of security." House Permanent Select Comm. on Intelligence, *Report of Russian Active Measures* 123 (March 22, 2018); *see also id.*

(emphasizing that "[t]he vulnerability of state and local election infrastructure has been well documented" and "[t]hese systems, which are not frequently updated or replaced, are not developed to defend against state-sponsored cyber threats").

Georgia is one of only five states that use paperless DRE machines for all voters, and the inherent deficiencies with paperless DRE machines have prompted states across the country to move away from the technology.[6] For example, just two months before the November 2017 election, Virginia decertified the paperless DRE machines used in 22 of its localities – including the Diebold AccuVote TSx. *See* Cortes, Commissioner of Virginia Dep't of Elections, Testimony to Subcomms. of U.S. House Comm. on Oversight and Gov't Reform 1, 3 (Nov. 29, 2017). "All affected localities promptly obtained new voting equipment" in the 59 days before the November 2017 election, and that election "was effectively administered without any reported voting equipment issues." *Id.* at 4. According to the Commissioner of Virginia's Department of Elections, "[t]he transition to

[6] The other states that use paperless DREs statewide are South Carolina, Delaware, New Jersey, and Louisiana. Voters in South Carolina just last week filed a lawsuit challenging that state's paperless-DRE-based voting system. *See* Monk, "SC's 13,000 voting machines unreliable, vulnerable to hackers, lawsuit alleges," *The State* (July 10, 2018). *Amicus* Protect Democracy represents the plaintiffs in that litigation. Eight other states (Arkansas, Indiana, Kansas, Kentucky, Mississippi, Pennsylvania, Tennessee, and Texas) use paperless DRE machines in some parts of the state. *See* Verified Voting, https://www.verifiedvoting.org/verifier/.

paper-based voting systems on a truncated timeline was incredibly successful and significantly increased the security of the election." *Id.* Similarly, in February 2018, Pennsylvania officials issued a directive requiring that all future purchases of voting machines must include the use of voter-verified paper ballots. *See* Media Advisory, "Wolf Administration Directs that New Voting Systems in the Commonwealth Provide Paper Record" (Feb. 9, 2018).

Georgia's voting system is especially vulnerable. Georgia uses an old model of Diebold AccuVote DREs that is less secure than the version found unacceptably vulnerable by many states over a decade ago. *See* TAC ¶¶59, 82; *supra* 5-6. Georgia is also the only state that uses Diebold's AccuVote paperless DRE statewide.[7] And its DREs run on an operating system that Microsoft stopped supporting with updates or security patches *over five years ago*. TAC ¶63.

Moreover, as described at length in the TAC, critical aspects of Georgia's voting system were left exposed to public access and manipulation between at least August 2016 and March 2017, and likely for a much longer period of time. TAC ¶¶95-106. Because of that public exposure, outsiders apparently *in fact accessed* files that included "voter histories and personal information of all Georgia voters,

[7] *See* Verified Voting, https://www.verifiedvoting.org/resources/voting-equipment/premier-diebold/accuvote-tsx/.

tabulation and memory card programming databases for past *and future elections*, instructions and passwords for voting equipment administration, and executable programs controlling essential election resources." TAC ¶97 (emphasis added).

In addition, shortly after Plaintiffs filed this lawsuit, the custodians of Georgia's election system wiped data from election servers that "could have revealed whether Georgia's most recent elections were compromised by hackers." Bajak, "APNewsBreak: Georgia election server wiped after suit filed," *APNews* (Oct. 27, 2017).[8] The documented outside access to critical components of Georgia's election system, together with the apparent loss of election system data that might have shown actual tampering or errors in Georgia's recent elections, makes Georgia unique and amplifies the already substantial risks caused by Defendants' reliance on an outdated paperless DRE voting system.

C. The threat that Georgia's voting system will be attacked in the upcoming election is real and serious

The risk that state voting systems will be attacked has increased dramatically in recent years. Georgia's unreliable and insecure voting system must be remedied immediately, given the substantial risk that it will be attacked in the next election.

[8] While paperless DREs are vulnerable to *undetectable* attacks, some kinds of hacking or errors could be discovered by review of election system data.

Evidence of past cyberattacks and the substantial threat of future attacks have been acknowledged by leaders throughout the intelligence and law enforcement communities. Just last Friday, Special Counsel Robert S. Mueller III issued an indictment against 12 Russian intelligence officers accusing them of extensive cyberattacks targeting the November 2016 election, including, among other things, "attempts to break into state elections boards." Mazzetti & Benner, "12 Russian Agents Indicted in Mueller Investigation," *New York Times* (July 13, 2018). The indictment specifically alleges that Russian agents "targeted state and county offices responsible for administering the 2016 elections." *United States v. Netyksho, et al.*, Indictment (D.D.C., July 13, 2018) ¶75.

According to the Senate Select Committee on Intelligence, "[i]n 2016, cyber actors affiliated with the Russian Government conducted an unprecedented, coordinated cyber campaign against state election infrastructure" in at least 21 states, "scanned databases for vulnerabilities, attempted intrusions," and in some cases "successfully penetrated a voter registration database." SSCI Report at 1. *See also* Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent US Elections, ICA 2017-01D* iii (Jan. 6, 2017) ("Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards."). And in recent testimony to Congress, Jeanette Manfra,

Assistant Secretary of the Office of Cybersecurity and Communications in the Department of Homeland Security, "acknowledged Russian hackers likely tried to hack into all 50 states." Levine, "Russia likely targeted all 50 states in 2016, but has yet to try again, DHS cyber chief says," *ABC News* (Apr. 24, 2018).

The threats to America's election infrastructure that emerged in 2016 have only increased. The U.S. intelligence community has confirmed that "[t]he risk is growing that some adversaries will conduct cyber attacks – such as data deletion or localized and temporary disruptions of critical infrastructure – against the United States in a crisis short of war," and in particular "[t]he 2018 US mid-term elections are a potential target …." Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community* 5, 11 (Feb. 13, 2018). In recent testimony to the Senate, the Directors of the CIA, FBI, NSA, Defense Intelligence Agency, and National Geospatial Intelligence Agency unanimously agreed "that Russia interfered in the 2016 election, and that the Kremlin *will continue to intervene in future elections*." Herb, "US intel chiefs unanimous that Russia is targeting 2018 elections," *CNN* (Feb. 13, 2018) (emphasis added). Indeed, "[i]n January 2018, the [then] Director of the Central Intelligence Agency [and now Secretary of State], Mike Pompeo, stated he has 'every expectation' Russia will continue meddling in U.S. elections, including the upcoming November 2018 midterm elections." Defending Digital

Democracy Project, Belfer Center, *The State and Local Election Cybersecurity Playbook* 8 (Feb. 2018) ("*Cybersecurity Playbook*"). And just last week, Director of National Intelligence Dan Coats said "that the persistent danger of Russian cyberattacks today [i]s akin to the warnings the United States had of stepped-up terror threats ahead of the Sept. 11, 2001, attacks. … 'The warning lights are blinking red again.'" Barnes, "'Warning Lights Are Blinking Red,' Top Intelligence Office Says of Russian Attacks," *New York Times* (July 13, 2018).[9]

Senior law enforcement officials have made similar assessments. Just last month, Deputy Assistant Attorney General Adam S. Hickey testified to Congress that the foreign operations that targeted the 2016 election "represent a significant escalation in the directness, level of activity, and scope of efforts aimed at the United States and our democracy, based in large part on the utility of the Internet for conducting these operations," and that the Department of Justice "is mindful of

[9] *See also* Johnson, former Secretary of Homeland Security, Statement to U.S. Senate Comm. on Intelligence (March 21, 2018) ("In 2016 the Russian government … orchestrated cyberattacks on our Nation for the purpose of influencing the election that year – plain and simple. … The matter is all the more urgent given the public testimony of our Nation's intelligence chiefs … that the Russians['] effort continues into the ongoing 2018 midterm election season."); Rosenbach, former Chief of Staff to the Secretary of Defense and Assistant Secretary of Defense for Homeland Defense and Global Security, Statement to U.S. Senate Comm. on Homeland Security and Governmental Affairs (April 24, 2018) ("[A]s we approach the 2018 midterm elections, the risk of Russian cyber and information attacks against our election systems and campaigns is very real.").

the [Office of the Director of National Intelligence's] assessment that Russia, and possibly other adversaries, *likely will seek to interfere in the 2018 midterm elections* …." Hickey, Deputy Assistant Attorney General, Statement to U.S. Senate Comm. on the Judiciary (June 12, 2018) (emphasis added). Operations targeting "voter registration databases and voting machines" and "aimed at removing otherwise eligible voters from the rolls or attempting to manipulate the results of an election (or even just disinformation suggesting that such manipulation has occurred) could undermine the integrity and legitimacy of elections, as well as public confidence in election results." *Id.* As explained by Eric Rosenbach, former Chief of Staff to the Secretary of Defense, "To succeed in destroying Americans' trust in democracy, Russia doesn't need to successfully attack the entire voting infrastructure. A cybersecurity incident in just a handful of counties could undermine public confidence in the national electoral process." Rosenbach, Statement to U.S. Senate Comm. on Intelligence (March 21, 2018).

Given this overwhelming documentation of the substantial imminent risks to our election infrastructure, the risk that Georgia's election system will be attacked in the upcoming election is far from hypothetical. Indeed, the recent indictment issued by Special Counsel Mueller specifically accused Russian operatives of "vist[ing] the websites of certain counties in *Georgia*, Iowa, and Florida to identify

vulnerabilities" as part of their broader conspiracy leading up the November 2016 election. *Netyksho* Indictment ¶75 (emphasis added). In addition, less than four months ago, the City of Atlanta was targeted in "one of the most sustained and consequential cyberattacks ever mounted against a major American city." Blinder & Perlroth, "A Cyberattack Hobbles Atlanta, and Security Experts Shudder," *New York Times* (March 27, 2018).[10]

The Atlanta attack is part of a recent global increase in cyberattacks. Last May, "North Korean hackers went after tens of thousands of victims in more than 70 countries around the world, forcing Britain's public health system to reject patients, paralyzing computers at Russia's Interior Ministry, at FedEx in the United States, and at shipping lines and telecommunications companies across Europe. [¶] A month later, Russian state hackers deployed similar ransomware to paralyze computers in Ukraine on the eve of the country's independence day." Blinder & Perlof. Research reflects that local governments are under a near-constant barrage of cyberattacks. *See* Norris, et al., "Local governments' cybersecurity crisis in 8 charts," *The Conversation* (April 30, 2018) (44% of local government respondents "told us they experience cyberattacks *at least daily*") (emphasis added).

[10] "[M]ore than a third of the city's 424 vital programs were kicked offline or disabled during the attack on March 22." Hogan, "City of Atlanta needs $9.5M to fund fallout from ransomware attack," *Atlanta Business Chronicle* (June 11, 2018).

Attacks against voting systems in the primaries running up to the November election have already begun. Two months ago, Knox County Tennessee suffered a cyberattack "that crashed a government website that displayed election results to the public during its primary election." Levine, "Tennessee Officials Are Trying to Get to the Bottom of an Election Night Cyberattack," *Huffington Post* (May 3, 2018). That attack was intentionally obvious, because it was designed as a smokescreen to hide a second attack that sought to extract data from county servers. *See* Whetstone, "Knox County election night cyberattack was smokescreen for another attack," *KnoxNews.com (USA Today Network)* (May 17, 2018). Because Georgia's paperless DREs are vulnerable to *undetectable* tampering, and because manipulating only a few votes in a few precincts could be enough to change a result in the November election, this Court should not expect – and cannot reasonably insist on – similar evidence of an actual attack on Georgia's election system before taking action.

Given that Georgia remains one of the few states that insists on using paperless DREs – and the accepted understanding that the November 2018 elections in Georgia will include close contests relevant to both the State and the Nation – the likelihood that Georgia will be attacked is very real. Such an event would cause irreparable harm to Plaintiffs and broadly undermine our democracy.

Relief before the November election is necessary to prevent that irreparable harm.

D. Georgia's voting system is unacceptably susceptible to undetectable errors in vote tallying even without malicious tampering

While the threat of manipulation is serious enough to warrant relief, Plaintiffs' claims do not rely on that threat alone. Even without tampering, electronic voting machines like those used in Georgia have caused errors in vote tallying in multiple past elections. Without a paper ballot, there will be no way to detect or correct such errors if they occur in the November 2018 election.

It is well-documented that "[t]ouch screen machines" like those used in Georgia "are vulnerable to 'calibration' problems, sometimes referred to as 'vote flipping,'" which "cause machines to register voters' choices for the wrong candidate. In recent elections, voters uploaded videos of this vote flipping to the Internet and they went viral." Norden & Famighetti, Brennan Center for Justice, *America's Voting Machines at Risk* 13-14 (2015) ("Brennan Center Report"). In the 2012 and 2014 federal elections, "news outlets documented calibration errors in Colorado, Illinois, Maryland, Nevada, North Carolina, Ohio, Pennsylvania, Texas, and Virginia." *Id.* These errors "become more frequent as machines age," *id.* at 13, and every Georgia county uses DRE machines that are *more than a decade old*. *See* Belt, "Georgia Counties with Ancient Voting Machines: Report," *Atlanta Patch* (Mar. 10, 2018).

Reports of vote tallying errors and other problems resulting from the use of DREs in past elections abound. Just a few examples follow:

a. "During the primaries in Florida in 2002, some machines in Miami-Dade malfunctioned and failed to turn on, resulting in hours long lines that locked out untold numbers of voters." Wofford, "How to Hack an Election in 7 Minutes," *Politico* (Aug. 5, 2016).

b. Later that year, "faulty software (and an administrator oversight) … led to a fourth of votes initially omitted during early voting in Albuquerque's Bernalillo County." *Id.*

c. "In Fairfax County, Virginia, an investigation into a 2003 school board race found that a vote was subtracted for every 100 votes cast for one of the candidates on 10 machines." *Id.*

d. "A malfunction of DREs in Carteret County, North Carolina, in the November 2004 elections caused the loss of more than 4,400 votes. There was no backup record of the votes that were cast." *Building Confidence in U.S. Elections* 25 (Sept. 2005) ("Carter-Barker Report"); *see* Associated Press, "More than 4,500 votes lost in North Carolina," *The Standard-Times* (Nov. 5, 2004). The race for Agricultural Commissioner was decided by fewer than the number of votes that were lost. The State Board of Elections called for a revote, but that proposal was struck down in court. Eventually one candidate conceded when the other candidate collected enough affidavits from voters claiming to have voted for him to ensure his election. *See* Jones & Simons at 312; Editorial, "Making Votes Count: One Last Election Lesson," *New York Times* (Jan. 18, 2005). Following this fiasco, Carteret County "abandoned its DREs," and "[o]ther jurisdictions have [similarly] lost votes because election officials did not properly set up voting machines." Carter-Baker Report at 26.

e. In 2006, the use of paperless DREs with insensitive touchscreens and a confusing ballot design led to an undervote rate of almost 13% in the House race in Sarasota County, Florida – and the specific causes of that extraordinary undervote rate were only understood some four years later, following extensive scrutiny. *See* Jones & Simons at 93, 119-22.

f. "In the 2008 Republican presidential primary in Horry County, South Carolina, touch screen voting machines in 80 percent of the precincts temporarily failed, and when precincts ran out of paper ballots, voters could not cast ballots in their home precinct." Goodman, et al., *Counting Votes 2012: A State by State Look at Voting Technology Preparedness* 3 (2012).

g. In 2011, officials in Cumberland County, New Jersey, were required by court order to *rerun an election* when it was discovered that the DRE machine used in the election had flipped the names of the candidates, recording each vote for one candidate as if it had actually been cast for the *other* candidate. Adomaitis, "Electronic voting case prompts new election, investigation in Fairfield," *NJ.com* (Sept. 2, 2011). Not surprisingly given the severity of this error, the rerun election resulted in different candidates being elected. Adomaitis, "Zirikles win Fairfield election; state can't confirm investigation," *NJ.com* (Sept. 27, 2011).

h. "In 2014, voters in Virginia Beach observed that when they selected one candidate, the machine would register their selection for a different candidate," because of an "alignment problem" with AccuVote TSx machines. Brennan Center Report at 13

The evidence of DRE-caused vote counting errors is not just anecdotal. Scholarly analysis reflects that DRE "residual vote rates" (i.e., the difference between the number of voters who voted and the number of ballots actually counted) are higher than the residual vote rates for optical scan and paper ballots. *See* Ansolabehere & Stewart, "Residual Votes Attributable to Technology," *The Journal of Politics*, Vol. 67, No. 2, at 366 (May 2005).

Courts have intervened in other circumstances when states used voting

systems that were unacceptably vulnerable to error.[11] And jurists in other countries have recognized that the substantial risks of undetectable, uncorrectable error caused by the use of paperless DRE voting machines makes the use of such machines incompatible with basic principles of democracy. In 2009, the German Federal Constitutional Court held unconstitutional a law permitting the use of paperless electronic voting machines that – like those in Georgia – offered no way to verify that votes were counted as cast, either by the voter in real time or through a later audit or recount. *See* BVerfG, Judgment of the Second Senate of 03 March 2009 - 2 BvC 3/07 ("BvC 3/07 Judgment") ¶147.[12] This Court, of course, is not

[11] *See, e.g. Stewart*, 444 F.3d at 848-50, 870 (use of punch card ballots with higher residual vote rates than other systems violated equal protection), *vacated as moot*; *Black v. McGuffage*, 209 F.Supp.2d 889, 899 (N.D.Ill. 2002) (denying motion to dismiss on similar grounds); *Common Cause v. Jones*, 213 F.Supp.2d 1106, 1107-08 (C.D. Cal. 2001) (similar); *Sw. Voter Registration Educ. Proj. v. Shelley*, 344 F.3d 882, 894-900 (9th Cir. 2003) (preliminary injunctive relief against use of punch card voting system justified by vote counting error rates), *vacated by* 344 F.3d 913, *reversed on other grounds by* 344 F.3d 914 (en banc) (reversing preliminary injunctive relief because election had already begun); *see also Bush v. Gore*, 531 U.S. 98, 104-05 (2000) ("Having once granted the right to vote on equal terms, the State may not … value one person's vote over that of another.").

[12] According to that court, "[a]n election procedure in which the voter cannot reliably comprehend whether his or her vote is unfalsifiably recorded and included in the ascertainment of the election result, and how the total votes cast are assigned and counted, excludes central elements of the election procedure from public monitoring, and hence does not comply with the constitutional requirements" of democracy. BvC 3/07 Judgment ¶113 (relying on foundational principles that Germany is a "democratic" state, that "[a]ll state authority is derived from the

bound by international decisions, but these jurists' thoughtfully reasoned conclusion that it is unacceptable in a democracy to use vulnerable voting machines like those used is Georgia deserves careful consideration.

E. Requiring paper ballots will substantially reduce the risk of undetectable, uncorrectable hacking or errors in the coming election

Plaintiffs' requested preliminary injunctive relief – that Defendants conduct Georgia's upcoming election using verifiable paper ballots, TAC ¶5 – is the only way to avoid the risk that undetectable tampering or errors will compromise the election. As explained by the nonpartisan experts at Harvard's Defending Digital Democracy Project: "To protect against cyber attacks or technology failures jeopardizing an election, it is essential to have a voter-verified auditable paper record to allow votes to be cross-checked against electronic results." *Cybersecurity Playbook* at 15.

> Without a paper vote record, accuracy and integrity of the recorded vote tally depends completely on the correctness and security of the machine's hardware, software, and data …. Any security vulnerability in this hardware or software, or any ability for an attacker to alter (or reload new and maliciously behaving) software running on a machine that does not produce a paper record, not only has the potential to alter the vote tally but can also *make it impossible to conduct a meaningful audit or recount (or even to detect that an attack has occurred)* after the fact.

---

people" and "shall be exercised by the people through elections," and that elections will be "free, equal, and secret," Basic Law of Germany, Arts. 20.1, 20.2, 38).

Id. (emphasis added). Paper ballots have allowed officials to catch critical errors in past elections. As just one example, "in Palm Beach County, Florida, in March 2012, a problem with election management software allotted votes to the wrong candidate and the wrong contest. The official results were only changed after a court-sanctioned public hand count of the votes." Goodman, et al. at 3.

To fully ensure that no tampering or software or administration errors compromise the election, statistically rigorous audits of the paper ballots should be conducted after the election. *See* Geller, Halderman, and Talbot-Zorn, "Here's how to keep Russian hackers from attacking the 2018 elections," *Washington Post* (June 21, 2017) ("[S]tates can gain high confidence regarding election outcomes by checking as few as 0.5 percent of the ballots in a given contest."). Such audits are not possible, however, if there are no paper ballots to check. Indeed, when the federal Election Assistance Commission asked the National Institute of Standards and Technology (NIST) to develop ways to audit a DRE-based voting system (i.e., "to verify that it has operated correctly in an election, and to identify the cause if it has not") that did *not* involve use of a paper ballot, the NIST's Auditability Working Group concluded that no such alternative is possible. *See* Report of the Auditability Working Group 5, 10 (Jan. 14, 2011).

Thus, if this Court does not grant preliminary relief ordering the use of

verifiable paper ballots, the only available remedy to address tampering or malfunctioning of Georgia's voting system – if it is detected – will be to *rerun the entire election*. *See supra* 21 (discussing court-ordered rerun of election in Cumberland County, New Jersey in 2011).

CONCLUSION

In seeking to dismiss the Coalition Plaintiffs' Third Amended Complaint and delay resolution of all Plaintiffs' anticipated motion(s) for preliminary injunctive relief, Defendants ask the Court to discount Plaintiffs' allegations as too speculative. That argument is inconsistent with the reality of election security and the very real threats facing Georgia's election infrastructure. The well-established risks associated with paperless DRE machines generally, the gaping security flaws in the particular Diebold system used in Georgia, the failures of Georgia officials to safeguard their system, and the substantial and imminent threats targeting American election infrastructure, combine to underscore the immediacy and urgency of Plaintiffs' constitutional claims. *Amici* respectfully urge the Court to give Plaintiffs' the opportunity to seek appropriate, full, and expeditious relief and then to grant that relief before the November election.

Date: July 17, 2018

Respectfully submitted,

By: s/ Jon L. Schwartz

JON L. SCHWARTZ (Ga. Bar No. 631038)
Jon L. Schwartz, Attorney at Law, P.C.
1170 Peachtree St. N.E., Suite 1200
Atlanta, Georgia 30309
Tel. (404) 667-3047
Fax (404) 529-4587

STEPHEN P. BERZON
(*pro hac vice* pending)
STACEY M. LEYTON
(*pro hac vice* pending)
MATTHEW J. MURRAY
(*pro hac vice* pending)
Altshuler Berzon LLP
177 Post Street, Suite 300
San Francisco, California 947108
Tel. (415) 421-7151
Fax (415) 362-8064

Attorneys for *Amici Curiae* Common Cause, National Election Defense Coalition, and Protect Democracy

CERTIFICATE OF COMPLIANCE

I certify that the foregoing Brief has been prepared in compliance with the font and point selections approved by the Court in LR 5.1C.

s/ Jon L. Schwartz

JON L. SCHWARTZ (Ga. Bar No. 631038)
Jon L. Schwartz, Attorney at Law, P.C.
1170 Peachtree St., N.E., Suite 1200
Atlanta, Georgia 30309
Tel. (404) 667-3047
Fax (404) 529-4587

CERTIFICATE OF SERVICE

I certify that I have this 17th day of July, 2018, served the foregoing Brief upon all counsel of record by way of the Court's electronic case filing (ECF) system.

s/ Jon L. Schwartz

JON L. SCHWARTZ (Ga. Bar No. 631038)
Jon L. Schwartz, Attorney at Law, P.C.
1170 Peachtree St., N.E., Suite 1200
Atlanta, Georgia 30309
Tel. (404) 667-3047
Fax (404) 529-4587