No. 2019-1204

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

FRANK HEINDEL; PHIL P. LEVENTIS,

Plaintiffs-Appellants,

v.

MARCI ANDINO, Executive Director of the South Carolina State Election Commission, in her official capacity; JOHN WELLS, Chair of the South Carolina Election Commission, in his official capacity; CLIFFORD J. ELDER, AMANDA LOVEDAY, SCOTT MOSELY, Members of the South Carolina State Election Commission, in their official capacity,

Defendants-Appellees.

Appeal from the United States District Court for the District of South Carolina at Columbia in No. 3:18-cv-1887-JMC, Judge J. Michelle Childs.

BRIEF OF *AMICI CURIAE* 13 ELECTION OFFICIALS IN SUPPORT OF PLAINTIFFS-APPELLANTS

Daniel A. Ladow
Magnus Essunger
Katherine Harihar
Gerald E. Porter
TROUTMAN SANDERS LLP
875 Third Avenue
New York, NY 10022
(212) 704-6000
daniel.ladow@troutman.com
magnus.essunger@troutman.com
katherine.harihar@troutman.com
gerald.porter@troutman.com

Lawrence Norden
Maximillian L. Feldman
Elizabeth Howard
Eliza Sweren-Becker
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
120 Broadway, Suite 1750
New York, New York 10271
(646) 292-8310

Counsel of Record for Amici Curiae

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 19-1204 Caption: *Heindel et al. v. Andino et al.*

Pursuant to FRAP 26.1 and Local Rule 26.1,

13 Election Officials
(name of party/amicus)

who is Amicus, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/ Katherine Harihar Date: 4/15/2019

Counsel for: 13 Election Officials

CERTIFICATE OF SERVICE

****

I certify that on April 15, 2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

s/ Katherine Harihar
(signature)

April 15, 2019
(date)

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases: **Page(s)**

Statutes

Other Authorities

STATEMENT OF INTEREST[1]

Amici curiae are current and former election officials from Arizona, California, Colorado, Florida, Kentucky, Michigan, New Mexico, New York, Pennsylvania, and Virginia. Collectively, *amici* are or were responsible for the administration of elections in eight cities or counties, and ten states.

Edgardo Cortés is the Former Commissioner of the Virginia Department of Elections, and is also the Former Chair, Vice Chair, and Secretary of the U.S. Election Assistance Commission ("EAC") Standards Board. As Commissioner, Mr. Cortés oversaw the 2015 decertification of WINVote Direct Recording Electronic ("DRE") voting machines and the 2017 decertification of all other paperless DRE voting systems in Virginia.

Lori Edwards is the Supervisor of Elections for Polk County, Florida, a position she has held since 2001. Ms. Edwards's office is responsible for administering all elections and providing support for municipal elections, as well as securing polling places, training election workers, and providing information on voter registration, voters, and elections.

[1] No party's counsel authored this brief in whole or in part. Neither any party nor any party's counsel contributed money that was intended to fund preparing or submitting this brief. No person other than *amici*, its members, or its counsel contributed money that was intended to fund preparing or submitting this brief. All parties have consented to the filing of this brief.

Adrian Fontes is the Recorder in Maricopa County, Arizona. The responsibilities of his office include maintenance of comprehensive public records and access to public records and voting information by the public. Mr. Fontes also oversees the voter registration, election administration activities and related security systems for a jurisdiction of approximately 2.5 million voters in the Phoenix metropolitan area of Maricopa County, Arizona.

Kammi Foote, Clerk-Recorder & Registrar of Voters in Inyo County, California, is a Member of the Board of Directors of the California Association of Clerks and Election Officials ("CACEO") and the Former Chair of the County Clerk Division of CACEO Legislative Committee. In 2017, Ms. Foote supervised her Inyo County's transition from DREs with a voter-verified paper audit trail to a paper ballot system.

Trey Grayson served as a two-term Secretary of State for the Commonwealth of Kentucky from 2004–11 and was President of the National Association of Secretaries of State and the Chair of the Republican Secretaries of State Association. He continues to be recognized as a national leader in election administration, including serving on the bipartisan Presidential Commission on Election Administration after the 2012 election and his ongoing work with several organizations to secure and modernize elections.

Hillary Hall served as Clerk and Recorder for Boulder County, Colorado from 2006 to 2018. During her tenure, the Clerk's office instituted processes to assist elections, such as same-day voter registration, mail balloting, and risk-limiting audits used to verify election results.

Tracy Howard is the General Registrar of Radford, Virginia and the Former President of the Voter Registrar Association of Virginia (2015–2017). Mr. Howard was responsible for securing funding for a new paper-based voting system in Radford and actively encouraged other localities to voluntarily transition to a paper-based system. Prior to Virginia's 2017 decertification of all paperless DREs, his support was an important factor in the voluntary transition by approximately 50 localities to voting systems which employ paper ballots.

Lisa Jeffers is the General Registrar of Waynesboro, Virginia. As General Registrar, Ms. Jeffers's responsibilities include aiding the State Board of Elections in preparations for all elections, certifying candidates and election winners, and maintaining the registered voter lists and election results. Ms. Jeffers is Former President of the Voter Registrar Association of Virginia (2013–2015). She has recognized and spoken about paperless election system equipment problems related to the aging and malfunctioning of paperless systems.

Douglas A. Kellner is the Co-Chair of the New York State Board of Elections, a position he has held since 2005. Mr. Kellner was one of the first

proponents of a voter verifiable paper audit trail for electronic voting machines and has been an outspoken advocate that the core principles for election administration should be accuracy, uniformity, transparency and verifiability.

Marian Schneider is the former Deputy Secretary for Elections and Administration in the Pennsylvania Department of State and formerly represented Pennsylvania on the EAC Standards Board. Ms. Schneider oversaw the Department's elections bureau during the 2016 presidential election cycle and issued guidance to Pennsylvania's 67 counties to harden their voting systems in advance of the election. She also advised Governor Tom Wolf on election security and developed a comprehensive set of recommendations to bolster the Commonwealth's election cyber security in 2017.

Linda Stover is the Bernalillo County Clerk in New Mexico. During her time as County Clerk, her office received a 2018 "Clearie" Award from the U.S. EAC in recognition of outstanding innovations in elections and best practices for recruiting, training, and accessibility of election workers, particularly Bernalillo County's "Learn the Vote" training program.

Chris Swope is the City Clerk of Lansing, Michigan, a position he has held since 2006. Mr. Swope was recently named to the Michigan Election Modernization Advisory Committee, which will advise the Michigan Secretary of

State on implementation of election reforms. He is the former President of the Michigan Association of Municipal Clerks (2014–2015).

Maggie Toulouse Oliver is the Secretary of State for New Mexico. She previously served as Bernalillo County Clerk from 2007 to 2016. Secretary Toulouse Oliver is committed to fair and efficient elections and increased voter access.

Amici are responsible for the day-to-day, year-round security of their respective election systems, and they are united in their dedication to securing the election systems in their respective jurisdictions. They are acutely aware that the integrity of our nation's elections is threatened by outside actors, as evidenced most prominently by Russian hacking of election systems in 2016, and by aging, malfunctioning paperless DRE election systems. Securing election systems and ensuring that every vote is counted as cast are critical components of their roles as election administrators. In today's heightened threat environment, *amici* believe that having a paper record of every vote is essential to election integrity, security, and reliability because it enables a meaningful audit or recount of the votes cast.

SUMMARY OF THE ARGUMENT

This appeal arises in the context of unprecedented security threats to election systems in the United States. In their experience as election administrators, *amici* know firsthand that threats to voting systems are numerous, pervasive, and pose a

substantial risk to election security and integrity for the foreseeable future. Given this current threat environment—which is widely acknowledged by U.S. national security, intelligence, and election agencies—*amici* also know that election officers are responsible for providing a minimum, reasonable level of security and implementing certain baseline measures to protect election integrity.

As alleged in the Complaint, South Carolina's current system, which is paperless and entirely digital, is highly vulnerable to hacking *and* prevents a meaningful audit of votes cast. Without a paper trail, election officials cannot implement effective measures to provide assurance to voters, including Plaintiffs, that their votes will be properly counted. *Amici* thus respectfully submit that the District Court erred in finding that Plaintiffs' alleged injury is overly "speculative" and not "fairly traceable" to Defendants. To the contrary, Defendants are aware of the real threats facing our election infrastructure and have not taken the most basic remedial step to prevent and recover from efforts to interfere with our elections by foreign adversaries—namely, adopting a system with a paper trail.[2]

[2] In the District Court, Defendants argued that a request for proposal by the Commission issued on December 7, 2018 for a system that includes a paper record of each vote should moot this action. However, it remains the case to date, as far as *amici* are aware, that South Carolina has neither committed to nor implemented a system having a paper trail.

ARGUMENT

I. PLAINTIFFS' INJURIES ARE SUBSTANTIALLY CERTAIN TO OCCUR AND FAIRLY TRACEABLE TO DEFENDANTS' CONDUCT

The District Court erred in concluding that Plaintiffs' theory of injury is too speculative and too attenuated to constitute an injury-in-fact.

Plaintiffs sufficiently allege that there is a substantial risk that their votes will not be properly counted for at least two reasons. First, given the history of efforts to attack South Carolina's election systems specifically, the myriad issues (e.g., vulnerability to hacking, malfunction, obsolescence) presented by South Carolina's aging paperless system, and the national threat environment, an attack on South Carolina's voting systems is certainly impending.[3] Second, South Carolina's system does not allow a meaningful audit of Plaintiffs' votes in recent and future elections. That means that Plaintiffs cannot be assured that their votes will be properly counted. *See Gray v. Sanders*, 372 U.S. 368, 380 (1963) ("Every voter's vote is entitled to be counted once. It must be correctly counted and reported."). These injuries compound one another: the threat to Plaintiffs posed by

[3] Given the Complaint's allegations and the national consensus about the magnitude and imminence of the threat, described in detail below, the District Court's finding of no standing is all the more erroneous because it appears to substitute the District Court's view of the risk for a reading of the Complaint's well-founded, clear allegations in the light most favorable to Plaintiffs as required in determining a motion to dismiss under Fed. R. Civ. P. 12(b). *See Battlefield Builders, Inc. v. Swango*, 743 F.2d 1060, 1061–62 (4th Cir. 1984).

the substantial risk of unauthorized access and election interference in South Carolina is exacerbated by Defendants' inability to ensure that every vote is counted as cast.

Plaintiffs' alleged harm is fairly traceable to Defendants' conduct because they are responsible for maintenance of the state's election system and they have failed to take the most basic remedial step to prevent and recover from efforts to interfere with our elections—implementing a more secure system that includes a paper trail. The paperless nature of South Carolina's current system precludes a meaningful audit of the votes cast and thus falls short of the minimum security baseline required by the present threat environment. Although a paper trail does not by itself preclude attacks by third parties, it remediates the impact of such attacks on voters, by enabling election officials to conduct a transparent review of votes cast and correct election outcomes, if necessary. Election administrators—including Defendants—have a responsibility to implement baseline security and integrity measures. Defendants may not abdicate this duty simply because it is undertaken in relation to the inevitable actions of third parties. By focusing for traceability purposes solely on the actions of third parties (e.g., would-be hackers) and disregarding the Commission's responsibility for the election system itself, the District Court erred.

A. Attacks On South Carolina's Election System Are Substantially Certain To Occur, Consistent With The Growing Nationwide Threat

The threat to our election infrastructure and systems has grown substantially over the last decade. Public revelations of Russian attempts to interfere in the 2016 election marked a turning point, demonstrating the gravity and sophistication of this growing threat and the vital role that election officials play in defending against efforts to undermine election integrity.

In this environment, it is not at all "speculative whether potential hackers will imminently target elections in South Carolina." *Heindel v. Andino*, 359 F. Supp. 3d 341, 353 (D.S.C. 2019). To the contrary, the State Election Committee ("SEC") reported to South Carolina's House Legislative Oversight Committee that the SEC blocked 149,832 attempts to penetrate the firewall of the statewide voter registration system on election day in 2016.[4] In the months that followed, the SEC rebuffed between 41,420 and 113,372 hacking attempts *per day*.[5] The SEC's director of public information and training explained that "events leading up to the 2016 General Election, including the breaches of other states' voter-registration

---

[4] *SEC Response to April 19, 2017 Executive Subcommittee Request for Additional Information* (Apr. 28, 2017), https://www.scstatehouse.gov/CommitteeInfo/HouseLegislativeOversightCommittee/AgencyWebpages/ElectionCommission/Letter%20from%20SEC%20to%20Oversight%20Subcommittee%20with%20attachments%20(April%2028,%202017).pdf

[5] *Id.*

systems, created an election-security environment that was very different[.]"[6] In other words, consistent with pervasive efforts to attack election systems nationwide, South Carolina has already been a target of attempted election interference. This specific experience, along with national threat assessments, all but ensure that South Carolina's election systems will continue to face attacks.

Federal government officials responsible for national security and intelligence are keenly aware that attacks on election systems and infrastructure are "certainly impending." For example, the Director of National Intelligence, Daniel R. Coats, said that "[t]he warning lights are blinking red again," comparing the danger of Russian cyberattacks today to pre-9/11 warnings about foreign attacks on U.S. soil.[7] Director Coats went on to state "[t]oday, the digital infrastructure that serves this country is literally under attack."[8] Last year, the U.S. Select Senate Committee on Intelligence confirmed that throughout 2016, "cyber actors affiliated with the Russian Government conducted an unprecedented, coordinated cyber

---

[6] Alexa Corse, *South Carolina May Prove a Microcosm of U.S. Election Hacking Efforts*, Wall Street Journal (July 16, 2017), https://www.wsj.com/articles/south-carolina-may-prove-a-microcosm-of-u-s-election-hacking-efforts-1500202806.

[7] *See* Jim Johnson, *'The Warning Lights Are Blinking Red Again,'* Brennan Center for Justice (July 16, 2018), https://www.brennancenter.org/blog/-warning-lights-are-blinking-red-again (hereinafter "The Warning Lights Are Blinking Red Again"); *see also* Worldwide Threat Assessment of the US Intelligence Community (Jan. 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[8] *See* The Warning Lights Are Blinking Red Again.

campaign against state election infrastructure."[9] *See* Complaint p. 36–38 ¶¶ 105–10. The Assistant Director for Cybersecurity for the Department of Homeland Security's ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA"), the DHS, and the Federal Bureau of Investigation ("FBI"), have acknowledged it is likely that every state was targeted.[10] Former Director of Central Intelligence, James Woolsey, commented that:

> [t]he history of national defense shows that threats are constantly evolving. When the United States was attacked at Pearl Harbor, we took action to protect our fleet. When we were attacked on 9/11, we took action to upgrade transportation security and protect our ports and other vulnerable targets. We were attacked in 2016. The target was not ships or airplanes or buildings, but the machinery of our

[9] *See* U.S. Select Senate Committee on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations* (May 8, 2018), https://www.intelligence.senate.gov/publications/russia-inquiry (hereinafter "Russian Targeting: Summary").

[10] *See* Mike Levine, *Russia likely targeted all 50 states in 2016, but has yet to try again, DHS cyber chief says*, ABC News (Apr. 24, 2018), https://abcnews.go.com/US/russia-targeted-50-states-2016-dhs-cyber-chief/story?id=54695520; Sean Gallagher, *DHS, FBI say election systems in all 50 states were targeted in 2016*, Ars Technica (Apr. 10, 2019), https://arstechnica.com/information-technology/2019/04/dhs-fbi-say-election-systems-in-50-states-were-targeted-in-2016/ (A joint intelligence bulletin recently issued by the DHS and the FBI indicated "The FBI and DHS assess that Russian government cyber actors probably conducted research and reconnaissance against all US states' election networks leading up to the 2016 Presidential elections.").

> democracy. We will be attacked again. We must act again—or leave our democracy at risk.[11]

Director Woolsey elaborated that the starting point for securing our elections includes "replac[ing] paperless electronic machines, upgrad[ing] the hardware and software that supports voter registration, and conduct[ing] post-election audits to confirm the results."[12]

In September 2018, former Secretary of Homeland Security, Kirstjen Nielsen, confirmed the threat posed by attempted interference by Russia in the U.S. voting process, noting that "[a]t Vladimir Putin's direction, Moscow launched a brazen, multi-faceted influence campaign to undermine public faith in our democratic process and to distort our presidential election."[13] Secretary Nielsen, recognizing that the government expects increasingly sophisticated attacks by foreign enemies, has further remarked that "[h]eightened aggression from cyber adversaries—including hostile nation states—is only accelerating in volume and sophistication," and, in noting the importance of working together to defend our

---

[11] *See* R. James Woolsey, *Securing Elections From Foreign Interference, Foreword*, Brennan Center for Justice (June 29, 2017), http://www.brennancenter.org/publication/securing-elections-foreign-interference.

[12] *Id*.

[13] *See* Secretary Kirstjen M. Nielsen Remarks: Rethinking Homeland Security in an Age of Disruption, Department of Homeland Security (Sept. 5, 2018), https://www.dhs.gov/news/2018/09/05/secretary-nielsen-remarks-rethinking-homeland-security-age-disruption (hereinafter "Secretary Nielsen Sept. 5th Remarks").

elections from the mounting risks, explained that "this is different than any threat we've seen before, because our democracy itself is in the crosshairs."[14] The threat of Russian attempts to interfere with U.S. elections was most recently confirmed by Attorney General William Barr in his summary of the report of Special Counsel Robert Mueller.[15]

Whatever the security situation was when paperless voting machines were introduced years ago, there is now a real and current threat to every state's election systems that is only becoming more urgent. The ongoing threat of interference is evidenced by actual breaches of voter and election related databases. In 2016, "hackers accessed a number of computer systems related to the election," including voter registration lists for Arizona and Illinois.[16] Attacks on voter registration

---

[14] *See* Secretary Kirstjen M. Nielsen Remarks to the National Election Security Summit, Department of Homeland Security (Sept. 10, 2018), https://www.dhs.gov/news/2018/09/10/secretary-kirstjen-m-nielsen-remarks-national-election-security-summit ("Don't underestimate the abilities of our adversaries. And don't assume you won't be affected by the next attempt. I assure you, they learn and get better.") (hereinafter "Secretary Nielsen Sept. 10th Remarks").

[15] Read Attorney General William Barr's Summary of the Mueller Report, N.Y. Times (Mar. 24, 2019), https://www.nytimes.com/interactive/2019/03/24/us/politics/barr-letter-mueller-report.html.

[16] U.S. EAC, Testimony, Before the Subcommittee on Information Technology of the Committee on Oversight and Government Reform (Sept. 28, 2016), https://www.eac.gov/assets/1/28/EAC%20Testimony%20before%20The%20Subcommittee%20on%20Information%20Technology%20of%20the%20Committee%20on%20Oversight%20and%20Governmnet%20Reform.pdf.

databases "have the potential to directly affect actual election operations."[17] After attending a briefing by officials from the FBI, DHS, and the National Security Agency, Steve Sandvoss, the Executive Director of the Illinois Elections Office, indicated that "[t]his was a first for me, . . . I came out of there with the understanding that the threat is not going to go away."[18] In Alaska, "state officials said an election-related server was scanned by Russian cyber-actors" a month before the 2016 election, and subsequently disclosed a "successful intrusion into the website-hosting server on Election Day."[19]

Cyberattacks are not simply one-time incidents. Nearly half of local governments reportedly experience cyberattacks at least daily, with many local governments reporting an increased or consistent number of attacks, incidents, or breaches from the past year.[20] Recognizing the need to work with state and local officials, the Department of Homeland Security formed a group of federal, state and local election officials and "beg[an] a program granting security clearances to

---

[17] *Id.*

[18] Eric Lichtblau, *'Our House Is on Fire.' Elections Officials Worry About Midterms Security*, Time (Sept. 5, 2018), http://time.com/5386422/election-security-midterms-russia/.

[19] Nathaniel Herz, *Hackers broke partway into Alaska's election system in 2016. Officials say no damage was done*, Anchorage Daily News (May 7, 2018), https://www.adn.com/politics/2018/05/07/hackers-broke-partway-into-alaskas-election-system-in-2016-officials-say-no-damage-was-done/#5088.

[20] *See* David Norris et al., *Local governments' cybersecurity crisis in 8 charts*, The Conversation (Apr. 30, 2018), https://theconversation.com/local-governments-cybersecurity-crisis-in-8-charts-94240.

state election officials" and also "expanded the agency's ability to conduct security reviews of state and local election systems for those that want them."[21]

That nationwide threat environment, along with specific efforts to penetrate South Carolina's election systems, demonstrate that Plaintiffs' injuries are certainly impending.

B. Securing Election Systems Against Unauthorized Access And Interference Is A Core Part Of Election Administration

Security has been a central feature of election administration for more than a century. In the current threat environment, the responsibilities of election administration include preventing, detecting, and mitigating third-party intrusion and manipulation of voting systems.

As far back as 1879, the Supreme Court upheld the constitutionality of federal election regulations, including legislation that required deputy marshals of the United States to "keep the peace and protect the [election] supervisors in the discharge of their duties[.]" *Ex parte Siebold*, 100 U.S. 371, 380 (1879); *see also Ex Parte Yarbrough*, 110 U.S. 651, 661 (1884) (recognizing that it cannot be doubted "that congress can, by law, protect the act of voting, the place where it is done, and the man who votes from personal violence or intimidation, and the

[21] Christina A. Cassidy, *'Russian playbook' remains after Mueller report wraps up*, Associated Press (Mar. 26, 2019), https://apnews.com/0c5961e9f88940e5949b261ed5942199.

election itself from corruption or fraud.").

More recently, Congress acknowledged the importance of security to election administration by allocating $380 million to the states to improve election security in March of 2018.[22] To accommodate each state's unique position on the election security spectrum, Congress created a list of six permissible expenditures for which the states could use this money.[23] "Replac[ing] voting equipment that only records a voter's intent electronically with equipment that utilizes a voter verified paper record" is first on the list.[24]

Every state and U.S. territory has requested their portion of this federal funding for election security.[25] The EAC provides dozens of resources for local election officials, including guidance on election security preparedness,[26] audits and recounts,[27] and cyber incident response best practices.[28]

---

[22] U.S. EAC, The Consolidated Appropriations Act of 2018 (Mar. 30, 2018), https://www.eac.gov/assets/1/6/2018_HAVA_Funds_background.pdf; U.S. EAC, *Help America Vote Act* ("HAVA"), https://www.eac.gov/about/help-america-vote-act/ (last visited Apr. 15, 2019).

[23] *See* U.S. EAC, *HAVA Funds State Chart View*, https://www.eac.gov/payments-and-grants/hava-funds-state-chart-view/ (last visited Apr. 15, 2019).

[24] *Id.*

[25] *Id.*

[26] *See* U.S. EAC, *Election Security Preparedness*, https://www.eac.gov/election-officials/election-security-preparedness/ (last visited Apr. 15, 2019) ("The U.S. EAC is working with all levels of government to facilitate the conversation regarding securing the election process and to support election officials' efforts to provide an accessible and secure voting process.").

[27] U.S. EAC, *Post-Election: Audits and Recounts*,

The federal government recently elaborated on the importance of state and local responsibility for election security, with former DHS Secretary Nielsen noting in late 2018 that "[e]lection security wasn't a mission we envisioned in the Department when it was created. But it's now one of my highest and continuous priorities. And in the past two years, we have worked hand-in-hand with state and local officials to make our election infrastructure more secure than ever."[29] DHS has also worked with local election officials "to set up an Election Infrastructure Information Sharing and Analysis Center (ISAC). This center is providing . . . election officials with timely and actionable information to help protect [their] systems."[30] Notably, "all 50 states and over 1,000 local jurisdictions have joined as members and are receiving this important information—making it the fastest growing ISAC in history—a testament to the commitment of election officials

---

https://www.eac.gov/election-officials/post-election-audits-recounts/ (last visited Apr. 15, 2019) ("While Election Day marks the end of voters casting ballots, state and local election officials still have a long to-do list to go through after the election. These include the many states that conduct post-election audits of voting systems as well as recounts that may occur in close races.").

[28] U.S. EAC, *Cyber Incident Response Best Practices*, https://www.eac.gov/assets/1/6/Incident-Response_best-practices.pdf ("U.S. EAC Best Practices") (last visited Apr. 15, 2019).

[29] Secretary Nielsen Sept. 5th Remarks.

[30] Secretary Nielsen Sept. 10th Remarks.

nationwide."[31]

DHS has confirmed that "[p]rotecting the 2020 election from hackers and foreign influence is a top priority," with the Director of DHS's CISA, Christopher Krebs, indicating that the agency was "doubling down" on its election security efforts for 2020.[32] A DHS senior adviser on election security, Matt Masterson, noted that these efforts by DHS would focus on local election officials, as security experts indicate that outreach, previously at the state level, "needs to zoom in on a county level."[33] Others have recognized the significant role of local election officials:

> There are about 8,800 county election officials across the US, and they are the people responsible for your voting machines, your polling place's security and handling vote auditing. "It may actually be the most important part of the entire infrastructure, these local county officials," said Jake Braun, executive director of the University of

---

[31] *Id.*; *see also* Elections Infrastructure-ISAC, 2018 Year in Review, https://www.cisecurity.org/wp-content/uploads/2019/02/EI-ISAC-2018-YIR.pdf (last visited Apr. 15, 2019) ("In the days leading up to and throughout the general election, 636 participants used the [National Cyber Situational Awareness Room] to report a variety of common malicious cyber activity, typosquatting, and even non-cyber physical threats.").

[32] Alfred Ng, *Homeland Security says it's 'doubling down' on 2020 election security efforts*, CNET (Feb. 14, 2019), https://www.cnet.com/news/homeland-security-says-its-doubling-down-election-security-efforts-for-2020/.

[33] Alfred Ng, *Election security in 2020 means a focus on county officials, DHS says*, CNET (Mar. 27, 2019), https://www.cnet.com/news/election-security-in-2020-means-a-focus-on-county-officials-dhs/.

> Chicago's Cyber Policy Initiative and co-founder of the Defcon Voting Machine Hacking Village.[34]

Attacks on our election systems are inevitable in 2020, according to the federal government itself.[35] Accordingly, the roles of election officials are critical to the protection of election security in our current environment.

C. In The Face Of Today's Heightened Threat To Election Infrastructure And Systems, Security Is A Feature Of Each Phase Of Election Administration

Election administrators have year-round security responsibilities that include, for example: physical and software maintenance of voting machines (e.g., regular equipment replacement, secure storage of machines, software auditing, and updates), voter list database maintenance (e.g., access limitations, encryption), and developing an incident response plan.

These election security measures are intended to prevent, detect, and recover from errors or manipulation that are possible at various times during an election cycle. Upkeep of non-networked voting machines limits the risks such machines are subject to since "chang[ing] a large number of votes typically requires access to the vote capture machine hardware or software, or the ability to introduce errors

---

[34] *Id.*

[35] Colleen Long & Michael Balsamo, *Cybersecurity officials start focusing on the 2020 elections*, Associated Press (Nov. 8, 2018), https://www.apnews.com/cfaa16f6a86349bebc16e0633d6214dd (Director Krebs said "[t]he big game we think for the adversaries is probably 2020.").

through the devices that program the vote capture device or download results from the vote capture device."[36] Protecting voter registration databases further secures the election process since an attacker connected to the database "can add, edit, or delete voters, allowing for false votes to be cast on election day or forcing voters to cast provisional ballots."[37] Developing responsive measures to attacks are an

---

[36] *See* Brian Calkin et al., *Handbook for Elections Infrastructure Security*, Center for Internet Security (Feb. 2018), https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf ("The consequences of a successful attack in a vote capture device are significant: the intentions of a voter are not properly reflected in the election results."); *see also* U.S. EAC, *Managing Election Technology: Ten Things To Know About Managing Aging Voting Systems* (Oct. 14, 2017), https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-managing-aging-voting-systems-voting-technology-voting-systems-cybersecurity/ ("States and jurisdictions are facing the prospect of continuing to manage aging voting systems in an environment in which expectations for security and reliability of these systems has never been greater.").

[37] Belfer Center for Science and International Affairs, *The State and Local Election Cybersecurity Playbook* (Feb. 2018), https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#practices ("Even if this does not affect actual vote outcomes, the perception of vote manipulation or voter suppression can significantly undermine the credibility of an election."); *see also* DHS, *Securing Voter Registration Data* (June 26, 2018), https://www.dhs.gov/sites/default/files/publications/Securing%20Voter%20Registration%20Data_508.pdf ("Malicious actors may use a variety of methods to interfere with voter registration websites and databases," with such attacks leading to credential theft, the spread of malware, theft of voter information or disruption of voting operations); U.S. EAC, *Checklist for Securing Voter Registration Data* (Oct. 23, 2017), https://www.eac.gov/documents/2017/10/23/checklist-for-securing-voter-registration-data/ ("State requirements for registration differ greatly, but every State maintains personally identifiable information associated with the voter's name to determine eligibility and precinct information. Due to the sensitive

important aspect in deterring and detecting security threats, such that federal agencies have recently become more involved in advising election officials on their responsibilities for preventing and addressing malicious attacks on their systems.[38]

In the weeks immediately preceding Election Day and on Election Day itself, election officials, such as the *amici*, implement additional election security measures designed to prevent and detect errors or manipulation, including pre-election day systems testing (including voting machines), and polling place security. Immediately following Election Day, election officials are also responsible for taking reasonable measures to detect errors or manipulation and correct initial election outcomes, if necessary. These measures can include canvasses, certifications, and audits.

D. In The Current Threat Environment, Baseline Security Requires Voting Machines That Produce A Paper Record And Allow For Post-Election Audits

In the current environment, two types of security practices are considered best practices to provide a minimum baseline of security for voting machines,

---

nature of this personal information, there is a natural concern on what security protocol has been used to secure the data.").

[38] *See* DHS, *Incident Handling Overview for Election Officials*, https://www.dhs.gov/sites/default/files/publications/Incident%20Handling%20Elections%20Final%20508.pdf (last visited Apr. 15, 2019); U.S. EAC, *Election Security Preparedness*, https://www.eac.gov/election-officials/election-security-preparedness/ (last visited Apr. 15, 2019).

specifically, (1) a paper record that, in turn, allows for (2) accurate, meaningful post-election audits.[39] The South Carolina voting machines at issue before the Court lack these essential security features. *See* Complaint p. 30–31 ¶¶ 83–88.

As noted above, Congress recognized the current failings of the American election systems and, through authorization under the Help America Vote Act ("HAVA"), allocated $380 million to the EAC as funding for States to "implement established cybersecurity best practices for election systems; and to fund activities that will improve the security of elections for federal office."[40] These practices are supported by national security, technology, and election officials, who clarified these requirements to various elected officers in an open letter, urging that state election officers:

> (1) Replace paperless voting machines with systems that count a paper ballot — a physical record of the vote that is out of reach from cyberattacks.
>
> (2) Conduct robust post-election audits in federal elections. Congress explicitly requested that states "implement a post-election audit system that provides a high-level of confidence in the accuracy of the

[39] *See* Secretary Nielsen Sept. 5th Remarks ("So to move the ball forward even more today, I am calling on every state in the Union to ensure that by the 2020 election, they have redundant, auditable election systems. *The best way to do that is with a physical paper trail and effective audits* so that Americans everywhere can be confident that—no matter what—their vote is counted and it is counted correctly.") (emphasis added).

[40] U.S. EAC, The Consolidated Appropriations Act of 2018 (Mar. 30, 2018), https://www.eac.gov/assets/1/6/2018_HAVA_Funds_background.pdf.

> final vote tally" as part of its report language accompanying the Omnibus . . . .[41]

That paper records are the minimum standard to be followed for election security has also been confirmed by the U.S. Select Senate Committee on Intelligence,[42] the DHS,[43] and the National Academies of Sciences, Engineering, and Medicine.[44] In 2018, then-House Intelligence Committee Chairman Devin Nunes called for a ban on electronic voting systems, urging that "we need a paper trail so that you can go back in case you have to do a manual recount,"[45] while

---

[41] *National Security, Tech, and Election Officials to States: Best Practices Should Guide How New Voting System Security Funds Are Spent* (Apr. 23, 2018), https://www.brennancenter.org/sites/default/files/analysis/Post-Omnibus_Sign-On_Letter_to_State_Election_Officials.pdf.

[42] Russian Targeting: Summary ("At a minimum, any machine purchased going forward should have a voter-verified paper trail and no WiFi capability.").

[43] Laura Hautala, *Homeland Security's tall order: A hacker-free election*, CNET (Feb. 23, 2018), https://www.cnet.com/news/homeland-securitys-tall-order-keep-hackers-out-of-the-next-election/ (DHS Assistant Director of Cybersecurity, Jeanette Manfra, stated, "I do believe that there should be audit capability and redundant means for checking if there is suspicion that something happened. And I know a lot of states and localities already have it, and if they didn't, they're working on it.").

[44] National Academies of Sciences, Engineering, and Medicine 2018, *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press, https://doi.org/10.17226/25120, at 80 ("Every effort should be made to use human-readable paper ballots in the 2018 federal election. All local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election.").

[45] Julie Manchester, *House Intel chair calls for ban on electronic voting systems*, The Hill (July 26, 2018), https://thehill.com/hilltv/rising/398949-house-intel-chair-calls-for-ban-on-electronic-voting-systems

former DHS Secretary Nielsen has said that not having a verifiable way to audit election results represents "a national security concern."[46]

South Carolina does not and cannot meet this minimum standard with its current voting system. Notably, the paperless iVotronic's alleged "audit system" simply compares the "tabulated results of the election with the raw data collected in the electronic audit files by each voting machine on a flash card."[47] *See* Complaint p. 30–31 ¶¶ 89–92. Such an "audit," which cannot be verified by an underlying paper record, is not an effective measure to assess whether each vote was counted as cast.

In evaluating what characteristics an auditable election system would possess, the Auditability Working Group of the National Institute of Standards and Technology ("NIST"):

> found no alternative that does not have as a likely *consequence* either an effective requirement for paper records or the possibility of undetectable errors in the recording of votes. If undetectable errors can be introduced at any point in the process, then the argument for

[46] Dustin Volz & Patricia Zengerle, *Inability to audit U.S. elections a 'national security concern': Homeland chief*, Reuters (Mar. 21, 2018), https://www.reuters.com/article/us-usa-trump-russia-security/inability-to-audit-u-s-elections-a-national-security-concern-homeland-chief-idUSKBN1GX200.
[47] The National Conference of State Legislatures, *Post-Election Audits* (Jan. 3, 2019), http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

> the correctness of the process as a whole inevitably has a missing link.[48]

Even if errors, manipulation, or machine failure is detected when using a paperless DRE machine, without a paper trail there is no effective means to ensure that every vote was counted as cast or to recover lost votes. For example, paperless DRE voting systems have been identified as the source of votes irretrievably lost or miscounted in New Jersey,[49] North Carolina,[50] and Virginia.[51] In South Carolina,

---

[48] NIST, *Report of the Auditability Working Group* (Jan.14, 2011), https://www.nist.gov/document-7152; *see also* NIST, *NIST Activities on UOCAVA Voting*, https://www.nist.gov/itl/voting/nist-activities-uocava-voting (last visited Apr. 15, 2019) (research by NIST later concluded that secure internet voting is not currently feasible).

[49] Greg Adomaitis, *Electronic voting case prompts new election, investigation in Fairfield*, NJ.com (Sept. 1, 2011), https://www.nj.com/cumberland/2011/09/touch-screen_voting_case_promp.html (New Jersey Superior Court voided election conducted on paperless DREs, with the judge stating, "I have my suspicions that something that happened here was improper," and that he did not "and may never" know, what exactly took place).

[50] *See E-Vote Machines Drop More Ballots*, Wired (Feb. 9, 2004), https://www.wired.com/2004/02/e-vote-machines-drop-more-ballots/ ("Six electronic touch-screen [iVotronic] voting machines used in two North Carolina counties lost 436 ballots cast in early voting for the 2002 general election because of a software problem."); *One Last Election Lesson*, N.Y. Times (Jan. 18, 2005), https://www.nytimes.com/2005/01/18/opinion/one-last-election-lesson.html ("The state has been unable to swear in an agriculture commissioner because a single malfunctioning electronic voting machine lost more ballots [(4,438)] than the number of votes that separate the two candidates. . . . The mess North Carolina finds itself in is a cautionary tale about the perils of relying on electronic voting that does not produce a paper record.").

[51] *See* Virginia Department of Elections, Interim Report on Voting Equipment Performance, Usage, and Certification (2015), https://www.wired.com/wp-content/uploads/2015/08/Virginia-Interim-Report-on-WINVote-Systems.pdf (one

votes are routinely collected and counted on paperless iVotronics even if the terminal indicates a malfunction.[52] *See* Complaint p. 22–25 ¶¶ 67–74, p. 30–31 ¶¶ 83–93.

As no election system is perfect, a paper record of every vote cast serves as an essential election security tool for election officials—and voters. These source documents can and have bolstered the public's confidence in our electoral system even when the original reported election outcome changed. For example, a recount of paper ballots corrected the vote totals in a delegate election which determined control of the Virginia House of Delegates in an election held *less than 60 days* after the state decertified all paperless DREs.[53] Similarly, a recount of paper ballots

---

vote irretrievably lost on a paperless voting machine in Virginia in 2014 Primary Election).

[52] *See* League of Women Voters of South Carolina, *Analysis of the Election Data from the 6 November 2018 General Election in South Carolina*, (Jan. 3, 2019), http://www.lwvsc.org/files/buell-lwvscreport2018scelection.pdf ("We continue to be concerned that votes are collected and counted iVotronic terminals that declare themselves to be malfunctioning, although we see no good remedy for this. To choose not to count votes from iVotronics with errors is to disenfranchise the voters who were directed to those iVotronics. To choose to count the votes is deliberately to include votes that might not be cast as intended. We believe this highlights the problem of using computers for elections when there is no means for determining ground truth and no backup capability.").

[53] *See* Kevin Robillard, *Virginia recount now tied with state House control in the balance*, Politico (Dec. 20, 2017), https://www.politico.com/story/2017/12/20/virginia-house-of-delegates-control-tied-308657.

in the 2016 City of Fairfax municipal election changed the election outcome.[54] Such corrections are not possible when using paperless DREs and the inability to conduct transparent and effective reviews of votes cast negatively impacts voters' confidence in our electoral system.

Therefore, a minimum security baseline for every voting system is to have a paper record that can be audited. Such a baseline enables election officials to conduct an essential bookend to the security measures implemented during the election cycle, a meaningful review of votes cast, and is strongly supported by national security, technology, and election officials. South Carolina's system does not meet that essential requirement.

[54] *See* Caroline Boras, *Fortunes reversed in Fairfax City Council vote recount*, Fairfax County Times (June 9, 2016), http://www.fairfaxtimes.com/articles/fortunes-reversed-in-fairfax-city-council-vote-recount/article_c7493ad2-2e7b-11e6-9f24-0732b2c2dd3c.html.

CONCLUSION

For the foregoing reasons, the Court should reverse the District Court's order and remand.

Respectfully submitted,

s/ *Katherine Harihar*
Daniel A. Ladow
Magnus Essunger
Katherine Harihar
Gerald E. Porter
TROUTMAN SANDERS LLP
875 Third Avenue
New York, NY 10022
(212) 704-6000
daniel.ladow@troutman.com
magnus.essunger@troutman.com
katherine.harihar@troutman.com
gerald.porter@troutman.com

Lawrence Norden
Maximillian L. Feldman
Elizabeth Howard
Eliza Sweren-Becker
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
120 Broadway, Suite 1750
New York, New York 10271
(646) 292-8310

Counsel of Record for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of *Amici Curiae* in Support of Appellants complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) and Fed. R. App. 29(a)(5) because this brief contains 6,087 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This Brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in proportionally spaced typeface using Microsoft Word 2016, the word processing system used to prepare the brief, in 14 point Times New Roman font.

Dated: April 15, 2019

Respectfully submitted,

s/ *Katherine Harihar*
Katherine Harihar
TROUTMAN SANDERS LLP
875 Third Avenue
New York, NY 10022
(212) 704-6000
katherine.harihar@troutman.com

Counsel of Record for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system on April 15, 2019.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: April 15, 2019

s/ *Katherine Harihar*
Katherine Harihar
TROUTMAN SANDERS LLP
875 Third Avenue
New York, NY 10022
(212) 704-6000
katherine.harihar@troutman.com

Counsel of Record for Amici Curiae