IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

Frank Heindel and Phil Leventis, Plaintiffs, v. Marci Andino, *Executive Director of the South Carolina State Election Commission, in her official capacity*; Billy Way, Jr., *Chair of the South Carolina State Election Commission, in his official capacity*; Mark A. Benson, Marilyn Bowers, and Nicole Spain Wright, *Members of the South Carolina State Election Commission, in their official capacity*, Defendants.	Civil Action No.: 3:18-cv-01887-JMC **ORDER AND OPINION**

Before the court for review is a Motion for Summary Judgment[1] (ECF No. 5) by Defendants Marci Andino, Executive Director of the South Carolina State Election Commission ("SCSEC"); Billy Way, Jr., Chair of the SCSEC; and Mark A. Benson, Marilyn Bowers, and Nicole Spain Wright, Members of the SCSEC (collectively "Defendants" or "SCSEC"). Defendants move the court to dismiss Plaintiffs Frank Heindel and Phil Leventis' (collectively "Plaintiffs") declaratory judgment action for lack of standing. For the reasons that follow, the court **GRANTS** Defendants' Motion.

[1] Although Defendants' Motion is titled "Motion for Summary Judgment," they request both summary judgment under Federal Rule of Civil Procedure 56 and dismissal under Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure. (ECF No. 5 at 1.) In their Response to Defendants' Motion, Plaintiffs argue that Defendants did not meet the requirements necessary for summary judgment. (ECF No. 14 at 38.) At a hearing on Defendants' Motion, Defendants expressed to the court that they only sought dismissal. (ECF No. 49 at 13:14–18.) Accordingly, the court construes Defendants' Motion only as a motion to dismiss.

I. FACTUAL AND PROCEDURAL BACKGROUND

Plaintiffs are "South Carolina voters seeking to vindicate their right to participate effectively in the state's elections." (ECF No. 1 at 3 ¶ 7.) On July 10, 2018, Plaintiffs filed a Complaint for Declaratory and Injunctive Relief, claiming that "the capacity of [South Carolina]'s election system to record and count votes reliably is deeply compromised by the state's" use of the iVotronic Direct Recording Electronic (DRE) system. (*Id.* at 2 ¶ 2.) After a Request for Proposal ("RFP")[2] in 2003, the SCSEC obtained 11,000 iVotronic voting machines from Electronic Systems & Software ("ES&S") for $35 million dollars. (*Id.* at 7–8 ¶¶ 22–23.) By 2006, the machines were in use statewide. (*Id.* at 8 ¶ 23.)

In their Complaint, Plaintiffs explain how the iVotronic DRE voting machines work:

> The iVotronic system consists of several components. The physical components—its "hardware"—include the following:
>
> - Voting terminals, which are computer systems that include touchscreens where users indicate their votes;
> - Personalized Electronic Ballots ("PEBs"), which are plastic cartridges housing infrared scanners that poll workers insert into the machines to open (or activate) the machines at the beginning of voting, close (or deactivate) the machines at the end of voting, make the correct ballot appear for each voter, and collect votes stored on the machine; and
> - Compact flash cards that store image files and an event log . . . from each machine. . . .
>
> The system also includes two software systems. The main one is iVotronic firmware—permanent software programmed into read-only memory—that directs the recording and tabulating of votes within the machines. The firmware creates

[2] The South Carolina Code defines a "Request for Proposal" as

> a written or published solicitation issued by an authorized procurement officer for proposals to provide supplies, services, information technology, or construction which ordinarily result in the award of the contract to the responsible bidder making the proposal determined to be most advantageous to the State. The award of the contract must be made on the basis of evaluation factors that must be stated in the RFP.

S.C. Code Ann. § 11-35-310(28) (West 2019).

the screen each voter sees as she scrolls through her electronic ballot. All of South Carolina's iVotronic machines utilize iVotronic firmware version 9.1.6.2, which the [SC]SEC certified in August 2006.

A second software system, Unity, works in conjunction with the machines' iVotronic firmware. Unity, an interconnected set of Windows-based software applications, runs on the counties' and [SC]SEC's server systems to translate the data captured via the iVotronic firmware into election results by county as well as statewide.

The process of voting on the iVotronic system is entirely digital. The user stands at the terminal, which presents the user's choices for each race or ballot question on a touchscreen; the user then votes by pressing the touchscreen to select and submit her choice. At no point in the process does the user create or receive a paper record reflecting her vote.

On Election Day, counties supply each precinct with one "red stripe" (also referred to as "master" or "supervisor") PEB and several "green stripe" (also referred to as "voter" or "ordinary") PEBs. Poll workers use the master PEB to open each terminal at the beginning of the day and close the terminals once voting ends. When closing voter terminals, the master PEB downloads and stores the vote totals collected over the course of the day in each machine. Poll workers then transport the master PEBs back to county elections headquarters, where officials transfer the results from the master PEBs to the Election Report Manager, a software system that tallies county-wide vote totals.

The "voter" PEBs serve a different role. Each time a voter checks in to vote, a poll manager uses a voter PEB to activate a terminal for that voter's use. The voter PEB prompts the terminal to show the proper ballot on the touchscreen and allows the user to vote once.

Each voter terminal also houses a compact flash card. The flash card is a removable electronic storage device, like a thumb drive or USB. Over the course of Election Day, the flash card stores "vote image files," digital records of ballots cast on that machine, and the selections made during completion of that ballot. The flash card also stores an event log showing what operations voters and poll workers caused the machine to execute over the course of the day. Operations include opening the machine, selecting a candidate, changing a selection, submitting a ballot, and closing the machine at the end of voting.

At county elections headquarters and the [SC]SEC, election officials employ the Unity system to create and manage election databases, design ballots, program the PEBs, and tabulate election results. The [SC]SEC certified Unity version 3.0.1.1 in August 2006. In 2014, the [SC]SEC certified Unity version 3.4.1.1. In 2017, it certified Unity version 4.0.0.3v4.

(*Id.* at 8–10 ¶¶ 24–31.)[3]

Plaintiffs allege that, "The iVotronic system is plagued with vulnerabilities that undermine its reliability and open numerous pathways for potential hacking." (*Id.* at 12 ¶ 38.) In support of their claim, Plaintiffs cite several reports that studied the same iVotronic voting machines and software in use in South Carolina. The first is a 2007 report commissioned by the Ohio Secretary of State entitled, "EVEREST: Evaluation and Validation of Electronic-Related Equipment, Standards and Testing."[4] (*Id.* at 13 ¶ 39.) The EVEREST Report concluded that the iVotronic system

> lack[s] the fundamental technical controls necessary to guarantee a trustworthy election under operational conditions. Exploitable vulnerabilities allow even persons with limited access—voters and precinct poll workers—to compromise voting machines and precinct results, and, in some cases, to inject and spread software viruses into the central election management system.

(*Id.* at ¶ 40 (quoting EVEREST Report at 29).) Plaintiffs further allege that, "The architecture of the iVotronic system creates numerous inroads for potential hackers," and the fact that the machines are not connected to the Internet does not insulate the system from attacks. (*Id.* at 16 ¶ 50 (citing EVEREST Report at 57).) For example, Plaintiffs assert that the PEBs, which are used to open and close the voting system, can transfer viruses to the iVotronic machines and to the central server with widespread and potentially undetectable consequences for the entire county's election process. (*Id.*) Plaintiffs argue that the security flaws identified by the EVEREST Report

---

[3] Defendants do not contest Plaintiffs' description of how the iVotronic machines operate. (ECF No. 5-1 at 11.)

[4] Pennsylvania State University, the University of Pennsylvania, WebWise Security, Inc., *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards, and Testing* (2007), https://www.eac.gov/file.aspx?D=pMbpd0z%2ffZc9yPf0v4FiM9f1TnszrIZM3FFSh9GsRLc%3d&A=AEsRG0%2bi8ImfT5LUBo4RN5dL8n3Npumes67vloL1mxI%3d [hereinafter "EVEREST Report"].

are not just theoretical because the EVEREST researchers performed several simulated attacks.[5] (*Id.* at 17 ¶ 52.)

In addition to the EVEREST Report, Plaintiffs cite a report commissioned by the South Carolina General Assembly ("General Assembly") to review the iVotronic system. (*Id.* at 19 ¶ 58.) In March 2013, the General Assembly's Legislative Audit Council ("LAC") published "A Review of Voting Machines in South Carolina," a study commissioned by the South Carolina Senate's President Pro Tempore.[6] (*Id.*) In addition to various "Election Day mishaps" associated with the iVotronic system, the 2013 LAC Report catalogued studies revealing the iVotronic's "deep and systematic vulnerabilities, including the EVEREST . . . report[]." (*Id.*)

In 2015, the General Assembly passed legislation establishing a "Joint Voting System Research Committee." (*Id.* at 19–20 ¶ 59.) This Joint Committee found "[a] new voting system must include some type of audit function, or 'paper trail,' that would allow the voter to confirm his or her ballot, as it will be tabulated by the [SC]SEC." (*Id.* at 20 at ¶ 59 (quoting 2013 LAC Report at 6).) The Joint Committee also held two public hearings in preparing its report. (*Id.* at ¶

---

[5] Plaintiffs also cite a 2017 report produced by computer security researchers at the annual DEFCON Hacking Conference. (ECF No. 1 at 21 ¶ 63.) According to Plaintiffs,

> Participants [at the DEFCON conference] had access to several electronic voting systems and searched for security breaches they could exploit. The equipment present at the DEFCON conference was available legally from secondary market sources, such as eBay, and participants did not receive access to source code. In other words, the participants faced constraints that might not apply to actual hackers, who could potentially obtain a broader array of machinery or source code. Among the machines included in the Voting Machine Hacking Village was the iVotronic voting machine and its associated PEB devices.

(*Id.*)

[6] South Carolina General Assembly Legislative Audit Council, *A Review of Voting Machines in South Carolina* (2013), https://www.scvotes.org/files/A%20Review%20of%20Voting%20Machines%20in%20SC%20%28Full%29.pdf [hereinafter "2013 LAC Report"].

60.) At the second hearing, Defendant Andino submitted testimony that South Carolina's current voting system has a life expectancy of twelve to fifteen years, and is approaching "end of life." (*Id.* at ¶ 61 (quoting 2013 LAC Report at 9).) Defendant Andino also reported that ES&S, the state's iVotronic machine vendor, informed the [SC]SEC that securing replacement parts "will become a problem at some time in the future." (*Id.*) Moreover, Plaintiffs assert that "ES&S no longer manufactures the outdated iVotronic machines." (*Id.*)

Plaintiffs further allege that the iVotronic "machines have failed in ways that impede voting," including:

> (1) a 2005 election in which machines in Myrtle Beach repeatedly malfunctioned and caused the supply of emergency paper ballots to be "running out"; (2) a 2005 city council primary race in Columbia which initially showed 3,208 total votes, but in which a manual recount revealed only 768 actual votes; and (3) a 2012 Richland County election in which widespread machine breakdowns caused massive delays, leaving voters waiting in line to vote as late as 11:30 p.m. [2013] LAC Report at 13. And in April 2018, *twelve* voting machines being used in a Goose Creek municipal election broke down with an unresolvable error.

(*Id.* at 22–23 ¶ 68.) Additionally, Plaintiffs allege that during the June 2018 primary elections,

> voting machines malfunctioned across the state, causing lines at the polls and delaying election results. In Greenville County, 33 voting machines at four precincts stopped working. As a result, lines to vote exceeded an hour in at least one Greenville County precinct. This mass mechanical failure delayed the reporting of results and required poll workers to call in an ES&S technician to review the machines' backup storage devices. The ES&S employee, rather than South Carolina poll workers, retrieved votes from the affected machines. Voting machines also broke in Horry, Marlboro, and Florence Counties. Even when the machines did not breakdown entirely, election officials acknowledged that aging touchscreens made it more difficult for voters to make their selections.

(*Id.* at 24–25 ¶ 74.)

Plaintiffs also assert that "the [SC]SEC has been aware of serious deficiencies in the security practices observed by county election officials" for at least a decade. (*Id.* at 25 ¶ 75.) These deficiencies "are different from, and in addition to, the iVotronic system's inherent security

vulnerabilities." (*Id.*) For example, the 2013 LAC Report found that "'Computers connected to networks or telephone lines . . . could potentially be used from unsecured or unauthorized access' and poor practices regarding keys and security codes." (*Id.* at 25–26 ¶ 75 (quoting 2013 LAC Report at 14).) Plaintiffs also cite 2016 reports from the South Carolina National Guard Defensive Cyber Operations Element, the United States Department of Homeland Security ("DHS"),[7] and the South Carolina Department of Administration ("SCDA"), which found "widely varying levels of physical- and cyber-security vulnerabilities." (*Id.* at 26–27 ¶¶ 77–80.) The SCSEC remedied "in hours" two of the three critical infrastructure vulnerabilities identified by the SCDA report. (*Id.* at 27 ¶ 80.) Plaintiffs allege that "[t]hese security gaps and vulnerabilities reflect a deficient approach to cybersecurity at the [SC]SEC. . . . indicat[ing], at best, a belated patching of critical- and high-vulnerability flaws and demonstrate a history of weak cybersecurity initiatives." (*Id.* at 27 ¶ 82.)

Next, Plaintiffs assert that "[b]ecause it is not possible to prevent all malicious attacks on an election system, states must implement safeguards that mitigate the risk of hacking by preserving a record of voter intent, detecting potential attacks, and providing a method for remedying errors or anomalies caused by successful attacks." (*Id.* at 28 ¶ 83.) According to Plaintiffs, the appropriate safeguards are "robust and consistent audit procedures." (*Id.*) Plaintiffs contend that in South Carolina, "effective post-election audits simply are not possible" because there is no record of voter intent independent of the iVotronic system. (*Id.* at 29 ¶ 87.) The SCSEC's current audit system "compares various components of the iVotronic and Unity Systems to determine whether they are internally consistent." (*Id.* at 30 ¶ 89.) Thus, Plaintiffs argue the

[7] The DHS Report was a "cyber hygiene assessment of the [SC]SEC's website and office network." (*Id.* at 27 ¶ 79.)

current audit process would not detect any attack on the state's voting system that impacted various system components. (*Id.* ¶ 90.) According to the EVEREST Report, the iVotronic system "forms a loop," meaning "a hack could unfold consistently across the system's components and thereby elude any process designed to detect 'anomalies.'" (*Id.*) Thus, if a hack occurred, "the [SC]SEC's audit process would simply check the hacked system against itself." (*Id.*) Also, Plaintiffs allege that the SCSEC's audit process does not indicate any mechanism to investigate anomalies in the system. (*Id.* at 31 ¶ 91.) Additionally, the 2013 LAC Report found that "in many instances, local election officials believe they lack adequate time to conduct the [SC]SEC's prescribed audit procedures between election day and the statutory deadline to certify results." (*Id.*)

Finally, Plaintiffs contend that the prospect of attacks on our nation's election systems is "immediate and acute." (*Id.* at 31 ¶ 94.) Plaintiffs assert that "[f]ederal and state election officials broadly recognize that foreign actors attempted to interfere with the 2016 national elections and that they have the capability and intent to do so again in future elections." (*Id.* at 32 ¶ 95.) As evidence of this "immediate and acute" threat of attacks on our nation's election system, Plaintiffs point to the indictment of thirteen Russian nationals and three Russian entities in a federal district court in Washington, D.C., for interfering with the United States' political system. (*Id.* ¶ 96.) Plaintiffs note that "Russia's well-documented interference has included cyberattacks directed at the nation's election infrastructure." (*Id.* ¶ 97.)

Plaintiffs also cite reports by the Federal Bureau of Investigation ("FBI") and DHS on interference in America's elections. In August 2016, the FBI issued an alert entitled "Targeting Activity Against State Board of Election Systems," which reported that "[i]n late June 2016, an

unknown actor scanned a state's Board of Election website for vulnerabilities."[8] (*Id.* at 33 ¶ 98 (quoting 2016 FBI Alert).) The 2016 FBI Alert advised all states to "take several specific technical steps to guard against similar cyberattacks." (*Id.*) In a September 2016 press release,[9] DHS reported detecting "efforts at cyber intrusions of voter registration data maintained in state election systems." (*Id.* ¶ 99 (quoting DHS Press Release).) In February 2018, DHS further reported "that hackers working for Russia 'tested the systems in most states. In some they tried to infiltrate the system and failed, but in Illinois the systems were successfully breached.'"[10] (*Id.* at 35 ¶ 103 (quoting Graham, *How Russia Could Meddle in the US Mid-Term Elections*).) Plaintiffs also cite reports by the United States House of Representatives and Senate, which concluded, among other things, that (1) "state and local election infrastructure . . . are not developed to defend against state-sponsored cyber threats. . . . [And] state and local election authorities should consider building in additional redundancies to ensure an audit trail in the event of a compromise of the electronic voting systems,"[11] (*Id.* at 35–36 ¶ 104 (quoting HPSCI, *Report on Russian Active Measures* at 123)); and (2) "[a]t least 18 states had election systems targeted

[8] Federal Bureau of Investigation, Cyber Division, *Targeting Against State Board of Election Systems* (Aug. 18, 2016), https://publicintelligence.net/fbi-election-hacking/ [hereinafter "2016 FBI Alert"].

[9] *Statement by Secretary Johnson Concerning the Cybersecurity of the Nation's Election Systems*, News Archive, Department of Homeland Security (Sep. 16, 2016), https://www.dhs.gov/news/2016/09/16/statement-secretary-johnson-concerning-cybersecurity-nation%E2%80%99s-election-systems [hereinafter "DHS Press Release"].

[10] Chris Graham, *How Russia Could Meddle in the US Mid-Term Elections - And Why It's Too Late to Secure Them Now*, The Telegraph (Feb.14, 2018), https://www.telegraph.co.uk/news/2018/02/14/russia-could-meddle-us-mid-term-elections-late-secure-now/ [hereinafter "Graham, *How Russia Could Meddle in the US Mid-Term Elections*"].

[11] House Permanent Select Committee on Intelligence, *Report on Russian Active Measures* (March 22, 2018), http://fm.cnbc.com/applications/cnbc.com/resources/styles/skin/special-reports/pdfs/russian-active-measures.pdf [hereinafter "HPSCI, *Report on Russian Active Measures*"].

by Russian-affiliated cyber actors in some fashion."[12] (*Id.* at 36 ¶ 105 (quoting SSCI, *Russian Targeting of Election Infrastructure During the 2016 Election*).) The Senate report also found that "[p]aperless [DRE] voting machines . . . are at highest risk for security flaws." (*Id.* at 38 ¶ 109 (quoting SSCI, *Russian Targeting of Election Infrastructure During the 2016 Election*).)

As to Plaintiffs' claims, Plaintiffs contend that "[w]hile the Constitution does not require a state to guarantee perfect accuracy or impregnable safeguards in its election systems, [the Constitution] does require a level of reliability that votes will be accurately counted, and that voters will not face arbitrary and disparate treatment." (*Id.* at 43 ¶ 124.) Plaintiffs assert that "Defendants have violated Plaintiffs' fundamental right to vote in violation of the Fourteenth Amendment by failing to approve and adopt a voting system that meets reasonable security standards." (*Id.* at 42 ¶ 121.) Plaintiffs also contend "[t]he [SC]SEC has provided and maintained a voting system that places a severe burden on Plaintiffs' right to vote. The state's voting system, organized around the iVotronic system, is so intensely vulnerable as to violate Plaintiffs' due process right to have their votes effectively recorded and counted." (*Id.* ¶ 122.) Finally, Plaintiffs claim that in violation of the Equal Protection Clause of the Fourteenth Amendment, Defendants have "subjected each Plaintiff's vote to arbitrary treatment as the system does not ensure that all machines, precincts, and counties will record and tabulate votes equally and reliably." (*Id.* at 42–43 ¶ 123.)

Based on these allegations, Plaintiffs request that the court (1) "[a]ssume jurisdiction over this action"; (2) "[d]eclare that . . .Defendants' failure to provide an elections system that has basic safeguards to ensure that the Plaintiffs' votes are reliably and accurately counted violates

[12] Senate Select Committee on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations* (May 8, 2018), https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf [hereinafter "SSCI, *Russian Targeting of Election Infrastructure During the 2016 Election*"].

Plaintiffs' fundamental right to vote as protected by the 14th Amendment to the U.S. Constitution"; (3) "[e]njoin Defendants from maintaining an election system that fails to reliably record and tabulate votes"; (4) "[i]mpose injunctive relief requiring Defendants to ensure that Plaintiffs have access to a voting system that will reliably and accurately record their votes"; and (5) "[a]ward the Plaintiffs reasonable attorneys' fees and costs pursuant to 42 U.S.C. § 1988." (*Id.* at 44.)

On July 30, 2018, Defendants moved to dismiss Plaintiffs' Complaint under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). (ECF No. 5 at 1.) Defendants argue Plaintiffs do not have standing to bring this action because their alleged injury (1) is not "concrete and particularized" and "actual or imminent" and (2) is not traceable to Defendants' conduct. (ECF No. 5-1 at 7–9, 10–12.) On August 28, 2018, Plaintiffs filed a Memorandum in Opposition to Defendants' Motion for Summary Judgment and Motion to Dismiss. (ECF No. 14.) On August 30, 2018, Defendants filed a Reply to Plaintiffs' Opposition to Motion to Dismiss. (ECF No. 15.) On January 4, 2019, Defendants filed a Supplemental Memorandum in Support of Defendants' Motion for Summary Judgment and Motion to Dismiss. (ECF No. 43.) In this Supplemental Memorandum, Defendants argue that Plaintiffs' claims are moot as a result of a RFP[13] issued by the SCSEC on December 7, 2018. (*Id.* at 1–2.) Defendants argue

> the [c]ourt should dismiss this case because Plaintiffs lack standing. Defendants have issued an RFP for a new voting system, one with a paper record of each voter's selections, that effectively moots the case. Moreover, Plaintiffs lack standing to bring the suit because a favorable decision would not redress Plaintiffs' alleged injury. The [SCSEC] is currently bound by a web of statutes and regulations that dictate how a new voting system is to be procured and implemented. Indeed, as is evidenced by the recently issued RFP, this process is ongoing and will be completed before the upcoming 2020 primaries. Stated plainly, the [c]ourt does not need to issue an order compelling the [SCSEC] to obtain new voting machines—the process is well under way.

[13] South Carolina State Election Commission, *Request for Proposal* (Dec. 7, 2018), http://webprod.cio.sc.gov/SCSolicitationWeb/contractSearch.do?solicitnumber=5400016872 [hereinafter "RFP"].

(*Id.* at 15.) On January 11, 2019, Plaintiffs filed a Memorandum in Response to Defendants' Supplemental Memorandum. (ECF No. 45.) On January 15, 2019, the court held a hearing on Defendants' Motion to Dismiss. (ECF No. 48.)

II. LEGAL STANDARD

Under Article III, Section 2 of the United States Constitution, the jurisdiction of the federal courts is limited to "[c]ases" and "[c]ontroversies." In *Simon v. E. Ky. Welfare Rights Org.*, the United States Supreme Court stressed that, "No principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." 426 U.S. 26, 37 (1976). The doctrine of standing curtails the disputes before the court in accordance with this limitation. *See Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 157 (2014) ("The doctrine of standing gives meaning to these constitutional limits by 'identify[ing] those disputes which are appropriately resolved through the judicial process.'" (alteration in original) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992))). Standing implicates the court's subject-matter jurisdiction and may be challenged in a motion to dismiss under Rule 12(b)(1) of the Federal Rules of Civil Procedure. *See Wikimedia Found. v. Nat'l Sec. Agency*, 857 F.3d 193, 208 (4th Cir. 2017); *Beyond Sys., Inc. v. Kraft Foods, Inc.*, 777 F.3d 712, 715 (4th Cir. 2015).

"The party attempting to invoke federal jurisdiction bears the burden of establishing standing." *Miller v. Brown*, 462 F.3d 312, 316 (4th Cir. 2006). "For purposes of ruling on a motion to dismiss for want of standing, both the trial and reviewing courts must accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party." *Warth v. Seldin*, 422 U.S. 490, 501 (1975). "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we 'presum[e] that

general allegations embrace those specific facts that are necessary to support the claim.'" *Lujan*, 504 U.S. at 561 (quoting *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 889 (1990)). "Nevertheless, the party invoking the jurisdiction of the court must include the necessary factual allegations in the pleading, or else the case must be dismissed for lack of standing." *Bishop v. Bartlett*, 575 F.3d 419, 424 (4th Cir. 2009). "When a defendant raises standing as the basis for a motion under Rule 12(b)(1) to dismiss for lack of subject matter jurisdiction, . . . the district court 'may consider evidence outside the pleadings without converting the proceeding to one for summary judgment.'" *White Tail Park, Inc. v. Stroube*, 413 F.3d 451, 459 (4th Cir. 2005) (quoting *Richmond, Fredericksburg & Potomac R.R. Co. v. United States*, 945 F.2d 765, 768 (4th Cir. 1991)).

III. ANALYSIS

At the outset, the court recognizes that the right at issue in this case—the right to vote and have that vote counted—is "a fundamental matter in a free and democratic society." *Reynolds v. Sims*, 377 U.S. 533, 561–62 (1964). *See also id.* at 554 ("It has been repeatedly recognized that all qualified voters have a constitutionally protected right to vote and to have their votes counted."). "[V]oters who allege facts *showing disadvantage to themselves as individuals* have standing to sue." *Baker v. Carr*, 369 U.S. 186, 206 (1962) (emphasis added).

"To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010)). To be particularized, an injury "must affect the plaintiff in a personal and individual way." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan*, 504 U.S. at 560 n.1). "There must be some connection between the plaintiff and the defendant that '[ ]differentiate[s]' the plaintiff so that his injury is not 'common to all members of

the public.'" *Griffin v. Dep't of Labor Fed. Credit Union*, 912 F.3d 649, 655 (4th Cir. 2019) (quoting *United States v. Richardson*, 418 U.S. 166, 177 (1974)). "The fact that an injury may be suffered by a large number of people does not of itself make that injury a nonjusticiable generalized grievance," as long as "each individual suffers a particularized harm." *Spokeo, Inc.*, 136 S. Ct. at 1548 n.7.

In their response to Defendants' Motion to Dismiss, Plaintiffs state that their "standing to pursue the claims in this litigation is rooted in the injury they suffer by virtue of having to cast their ballots using the highly vulnerable, deeply deficient voting system Defendants certified and maintain in South Carolina." (ECF No. 14 at 18.) Generally, Plaintiffs contend the iVotronic machines are unconstitutionally vulnerable to (1) hacking and (2) failure. (ECF No. 14 at 17.) More specifically, Plaintiffs allege they are injured by (1) Defendants' "fail[ure] to approve and adopt a voting system that meets reasonable security standards"; (2) Defendants' "maint[enance] [of] a voting system [so intensely vulnerable] that [it] places a severe burden on Plaintiffs' right to vote"; and (3) Defendants "subject[ing] each Plaintiff's vote to arbitrary treatment as the system does not ensure that all machines, precincts, and counties will record and tabulate votes equally and reliably." (ECF No. 1 at 42–43 ¶¶ 121–23.)

Recently, in *Clapper v. Amnesty International USA*, the United States Supreme Court reviewed the requirements of Article III standing in the context of threatened injury or substantial risk of harm. 568 U.S. 398, 409 (2013). The *Clapper* Court reiterated that for a threatened injury to constitute an "injury in fact," it "must be *certainly impending*."[14] *Clapper*, 568 U.S. at 410

[14] The *Clapper* decision indicates that plaintiffs can prove an injury-in-fact by proving either that the threatened injury is "certainly impending," or that there is a "substantial risk of harm": "[T]o the extent that the 'substantial risk' standard is relevant and is distinct from the 'clearly impending' requirement, respondents fall short of even that standard, in light of the attenuated chain of

(emphasis added) (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). The Supreme Court further explained that,

---

inferences necessary to find harm here." *Clapper*, 568 U.S. at 414 n.5. A year after *Clapper*, in *Susan B. Anthony List v. Driehaus*, a pre-enforcement challenge to an Ohio statute, the Supreme Court again stated that an injury-in-fact can be shown when there is a substantial risk of harm. 573 U.S. 149, 158 (2014) ("An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a '"substantial risk" that the harm will occur.'" (quoting *Clapper*, 568 U.S. at 414 n.5)). Thus, the Supreme Court's decisions in *Clapper* and *Susan B. Anthony* indicate that plaintiffs can allege a future injury by showing either a substantial risk of harm or that the threatened injury is certainly impending. The United States Court of Appeals for the Fourth Circuit appears to have found the same. In *Beck v. McDonald*, which is post-*Clapper* and *Susan B. Anthony*, the Fourth Circuit analyzed a claim of increased risk of future identity theft under both the certainly impending and substantial risk of harm standards. *See* 848 F.3d 626, 275 (4th Cir. 2017) ("Nonetheless, our inquiry on standing is not at an end, for we may also find standing based on a 'substantial risk' that the harm will occur, which in turn may prompt a party to reasonably incur costs to mitigate or avoid that harm." (citing *Clapper*, 568 U.S. at 414 n.5)).

Significantly, neither *Clapper*, *Susan B. Anthony*, nor *Beck* define the difference between the two standards, making it difficult to say with particularity what a plaintiff must show to prove a substantial risk of harm. However, *Clapper* does state that "we have found standing based on a 'substantial risk' that the harm will occur, *which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm*." 568 U.S. at 414 n.5 (emphasis added). But, the *Clapper* Court offers no clues as to the force of the "reasonably to incur costs to mitigate or avoid that harm" language, and the Court did not repeat this language in *Susan B. Anthony*. *See Susan B. Anthony*, 573 U.S. at 158 ("'An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a '"substantial risk" that the harm will occur.'" (quoting *Clapper*, 568 U.S. at 414 n.5)). In *Beck*, the Fourth Circuit also uses the "reasonably to incur costs to mitigate or avoid that harm" language: "[W]e may also find standing based on a 'substantial risk' that the harm will occur, *which in turn may prompt a party to reasonably incur costs to mitigate or avoid that harm*." 848 F.3d at 275 (citing *Clapper*, 568 U.S. at 414 n.5 (emphasis added)). *See also Organic Seed Growers & Trade Ass'n v. Monsanto Co.*, 718 F.3d 1350, 1355 (Fed. Cir. 2013) ("Thus, the question in this case is not whether the appellants' subjective fear of suit by Monsanto is genuine, but whether they have demonstrated a '"substantial risk" that the harm will occur, which may prompt [them] to reasonably incur costs to mitigate or avoid that harm.'" (quoting *Clapper*, 568 U.S. at 414 n.5)). The Fourth Circuit also did not comment on the force of this language in *Beck*. Neither the Supreme Court nor the Fourth Circuit have indicated that the "reasonably to incur costs to mitigate or avoid that harm" language is dispositive or carries more weight in the substantial risk of harm inquiry. *See Susan B. Anthony*, 573 U.S. at 158; *Clapper*, 568 U.S. at 414 n.5; *Beck*, 848 F.3d at 275. *C.f. Organic Seed Growers*, 718 F.3d at 1355. Therefore, in determining whether Plaintiffs have shown a substantial risk of harm, this court will consider whether the risk is such that it would "prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm" just like any other considerations deemed relevant by caselaw. *Beck*, 848 F.3d at 275 (citing *Clapper*, 568 U.S. at 414 n.5).

> "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending." [*Monsanto Co.*, 561 U.S.] at 565, n. 2 . . . . Thus, we have repeatedly reiterated that "threatened injury must be *certainly impending* to constitute injury in fact," and that "[a]llegations of *possible* future injury" are not sufficient. *Whitmore,* 495 U.S., at 158 . . . (emphasis added . . .)."

Clapper, 568 U.S. at 409.

Initially, accepting as true the allegations in Plaintiffs' Complaint, the court finds Plaintiffs have shown that elections in America have been interfered with, the threat that American elections will be interfered with remains, and that the iVotronic voting machines in use in South Carolina are vulnerable to hacking. (*See* ECF No. 1 at 13 ¶ 40 (quoting EVEREST Report at 29), 16 ¶ 50 (citing EVEREST Report at 57), 30 ¶ 90, 31–35.) However, Plaintiffs fail to show that the alleged threatened injury—the possibility their vote will not be accurately counted due to a hack of South Carolina's voting machines is *certainly impending*.

First, it is speculative whether potential hackers will imminently target elections in South Carolina. *Cf. Clapper*, 568 U.S. at 411 ("First, it is speculative whether the Government will imminently target communications to which respondents are parties."). Plaintiffs' standing theory is substantially undermined by the fact that they do not allege that South Carolina's election system has ever been hacked or that any attempts have ever been made to hack it. *See id.* at 411 ("Accordingly, it is no surprise that respondents fail to offer any evidence that their communications have been monitored under § 1881a, a failure that substantially undermines their standing theory."). *Cf. Curling v. Kemp*, 334 F. Supp. 3d 1303, 1314 (N.D. Ga. 2018) ("[The d]efendants argue that [the p]laintiffs' allegations that the DRE voting machines are vulnerable to hacking and are 'presumed to be compromised' convey only a speculative, generalized fear, thus falling short of establishing a concrete injury. These arguments are unavailing. For one, [the p]laintiffs have alleged that the DRE voting system was *actually* accessed or hacked multiple times

already – albeit by cybersecurity experts who reported the system's vulnerabilities to state authorities, as opposed to someone with nefarious purposes.") Furthermore, while the reports cited by Plaintiffs undeniably answer whether or not the iVotronic system *can be* hacked, they do not answer whether South Carolina's iVotronic system *will be* hacked. (*See* ECF No. 1 at 13 ¶ 40 (quoting EVEREST Report at 29), 16 ¶ 50 (citing EVEREST Report at 57), 30 ¶ 90, 31–35.) For example, the Senate Report cited by Plaintiffs found that the election systems of eighteen states had been targeted by Russian-affiliated cyber actors. (ECF No. 1 at 36 ¶ 105 (quoting SSCI, *Russian Targeting of Election Infrastructure During the 2016 Election*).) However, Plaintiffs do not allege that South Carolina was among these states. (*See id.*) *Cf. Clapper*, 568 U.S. at 412 ("Respondents, however, have set forth no specific facts demonstrating that the communications of their foreign contacts *will be* targeted." (emphasis added)).

On this "will be" question, the court finds instructive a recent decision by the Fourth Circuit on standing in the context of an increased risk of future identify theft. In *Beck v. McDonald*,[15] the plaintiffs "sought to establish Article III standing based on the harm from the increased risk of future identity theft and the cost of measures to protect against it." 848 F.3d 262, 266–67 (4th Cir. 2017). The plaintiffs were "veterans who received medical treatment and healthcare" at a Veterans Affairs' medical center in Columbia, SC. *Id.* at 266. A report found that

---

[15] *Beck* involved two appeals consolidated by the Fourth Circuit. 848 F.3d 262, 269 n.3 (4th Cir. 2017). While the *Beck* plaintiffs' identity theft case was pending,

> Beverly Watson[, also a named plaintiff in *Beck*,] brought a putative class-action lawsuit on behalf of the over 2,000 individuals whose pathology reports had gone missing. Watson sought money damages and declaratory and injunctive relief, alleging the same harm as did the *Beck* plaintiffs. The [d]efendants moved to dismiss the complaint for lack of subject-matter jurisdiction and for failure to state a claim.

Id. at 268. The district court found that the plaintiffs lacked standing in both cases, which all plaintiffs appealed. *Id.* at 269.

> on February 11, 2013, a laptop connected to a pulmonary function testing device with a Velcro strip was misplaced or stolen from [the medical center]'s Respiratory Therapy department. The laptop contains unencrypted personal information of approximately 7,400 patients, including names, birth dates, the last four digits of social security numbers, and physical descriptors (age, race, gender, height, and weight).

Id. at 267. The *Beck* plaintiffs

> filed suit on behalf of a putative class of the approximately 7,400 patients whose information was stored on the missing laptop. Relevant to this appeal, the *Beck* plaintiffs sought declaratory relief and monetary damages under the Privacy Act, alleging that the "Defendants' failures" and "violations" of the Privacy Act "caused Plaintiffs . . . embarrassment, inconvenience, unfairness, mental distress, and the threat of current and future substantial harm from identity theft and other misuse of their Personal Information." J.A. 12. They further allege that the "threat of identity theft" required them to frequently monitor their "credit reports, bank statements, health insurance reports, and other similar information, purchas[e] credit watch services, and [shift] financial accounts." J.A. 12.

Id.

The Fourth Circuit held that "the [p]laintiffs' theory [wa]s too speculative to constitute an injury-in-fact." *Id.* at 274.[16] First, the court highlighted that the *Beck* plaintiffs did not allege "the data thief intentionally targeted the personal information compromised in the data breaches" or "misuse . . . of that personal information by the thief." *Id.* The court found the failure to make such claims, "render[ed] their contention of an enhanced risk of future identity theft too speculative." *Id.* Additionally, the court stated that "'as the breaches fade further into the past,'" the *Beck* [p]laintiffs' threatened injuries become more and more speculative." *Id.* at 275 (quoting *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 570 (D. Md. 2016)). Finally, the court concluded

[16] The court held the same for the *Watson* appeal. *See id.* at 275 ("Plaintiffs['] . . . claims . . . . of an enhanced risk of future identity theft [are] too speculative. On this point, the data breaches in *Beck* and *Watson* occurred in February 2013 and July 2014, respectively. Yet, even after extensive discovery, the *Beck* plaintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information. Watson's complaint suffers from the same deficiency with regard to the four missing boxes of pathology reports." (footnote omitted)).

that "the mere theft [of the laptop and pathology reports], without more, cannot confer Article III standing." *Id.*

Similarly, in this case, Plaintiffs allege Defendants' failures have caused Plaintiffs the threat of future injury from the hacking or malfunction of South Carolina's iVotronic voting machines. (ECF No. 1 at 42–43 ¶¶ 121–23, 44.) *Compare Beck*, 848 F. 3d at 267 ("[T]he *Beck* plaintiffs sought declaratory relief . . . alleging that the 'Defendants' failures' and 'violations' of the Privacy Act 'caused Plaintiffs . . . embarrassment, inconvenience, unfairness, mental distress, and the threat of current and future substantial harm from identity theft and other misuse of their Personal Information.' J.A. 12.") *with* (ECF No. 1 at 44 "Plaintiffs respectfully request that the [c]ourt . . . [d]eclare Defendants' failure to provide an elections system that has basic safeguards to ensure that the Plaintiffs' votes are reliably and accurately counted violates Plaintiffs' fundamental right to vote as protected by the 14th Amendment to the U.S. Constitution.").) According to the reports cited by Plaintiffs, the iVotronic voting machines maintained by the SCSEC have virtually always been vulnerable to hacking; the iVotronic machines were implemented in 2006, and the EVEREST Report on which Plaintiffs heavily rely was published in 2007. (ECF No. 1 at 8 ¶ 23, 12–13 ¶¶ 38–39, 19 ¶ 57.) But, like the *Beck* plaintiffs, Plaintiffs do not allege South Carolina's elections, or Plaintiffs' votes, are being targeted by potential hackers, have ever been targeted by potential hackers, or that there has ever been a hack, or an attempted hack, of South Carolina's election system. *See Beck*, 848 F.3d at 273–75; (ECF No. 1 at 1–3 ¶¶ 1–7). However, Plaintiffs also assert that "[t]he security risks inherent in the iVotronic system are made even more acute by the current threat environment," and "the [SC]SEC itself has acknowledged that events leading up to the 2016 election, including the breaches of other states' voter registration systems, 'created an election-security environment that was very different' than

it has been in the past." (ECF No. 14 at 15.) Still, even since 2016, Plaintiffs do not allege there has been a hack or attempted hack of South Carolina's election system or voter registration system. Certainly, "[o]ne does not have to await the consummation of threatened injury to obtain preventive relief." *Pennsylvania v. West Virginia*, 262 U.S. 553, 593 (1923). But, neither can litigants claim a certainly impending injury for an indefinite amount of time. *See Doe v. Obama*, 631 F.3d 157, 163 (4th Cir. 2011) ("The imminence requirement is 'stretched beyond the breaking point when, as here, the plaintiff alleges only an injury at some indefinite future time.'" (quoting *Lujan*, 504 U.S. at 565 n.2)). And as the "events leading up to the 2016 election," (ECF No. 14 at 15), "'fade further into the past[,]' . . . Plaintiffs' threatened injuries become more and more speculative." *Beck*, 848 F.3d at 275 (quoting *Chambliss*, 189 F. Supp. 3d at 570).

Additionally, like in *Clapper*, Plaintiffs' hacking theory of injury "relies on a highly attenuated chain of possibilities." *Clapper*, 568 U.S. at 410 ("[R]espondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending."). First, it is speculative whether hypothetical hackers—unidentified by Plaintiffs[17]—will imminently target *Plaintiffs' votes* cast *in South Carolina elections*, as Plaintiffs make no allegations that *their votes* have been targeted by potential hackers or will be so targeted. *See id.* at 410–11 ("First, it is speculative whether the Government will imminently target communications *to which respondents are parties*. Accordingly, it is no surprise that respondents fail to offer any evidence that *their communications* have been monitored under § 1881a, a failure that substantially undermines their standing theory." (citation omitted) (emphasis added)); *Stein v. Cortes*, 223 F. Supp. 3d 423, 432 (E.D. Pa. 2016) ("Although Mr. Reitz

[17] Plaintiffs' failure to identify who these hypothetical hackers are makes their future injury even more speculative. *Cf. Clapper*, 568 U.S. at 411 ("First, it is speculative whether *the Government* will imminently target communications to which respondents are parties." (emphasis added)).

is a Pennsylvania voter, he has not alleged that *his vote was inaccurately recorded or tallied in the final Pennsylvania vote count*."); *Stewart v. Blackwell*, 444 F.3d 843, 870–71 (6th Cir. 2006), *vacated and superseded by*, 473 F.3d 692 (6th Cir. 2007)[18] ("Although voters approach the polls with the opportunity to vote in the same elections for the same candidates, once they step into the voting booth, they have an unequal chance of their vote being counted, not as a result of any action on the part of the voter, but because of the different technology utilized. . . . voters using the two challenged technologies have an additional likelihood of disenfranchisement due to the inherent deficiencies of the punch-card and central-count optical scan." (emphasis added)); *Black v. McGuffage*, 209 F. Supp. 2d 889, 895 (N.D. Ill. 2002) ("The 'probabilistic' injury is particularly high for those named [p]laintiffs whose election precincts had particularly high residual vote rates."); *id.* at 899 ("That people in different counties have significantly different probabilities of having their votes counted, solely because of the nature of the system used in their jurisdiction is the heart of the problem."); *Schulz v. Kellner*, No. 1:07-CV-0943 LEK/DRH, 2011 WL 2669456, at *7 (N.D.N.Y. July 7, 2011) ("Moreover, even construing their Amended Complaint to mean that the machine error and human fraud resulting from [the d]efendants' voting procedures will also harm [the p]laintiffs—whose votes will allegedly not be counted accurately—the [c]ourt finds that these allegations are merely conjectural and hypothetical and do not demonstrate a concrete or particularized injury to [the p]laintiffs. [The p]laintiffs have not presented any concrete or specific factual allegations from which the [c]ourt could infer, for instance, that their votes were diluted, that they are being disfavored by a gerrymandering scheme, or that they were unfairly denied access to a polling station.").

[18] The opinion was vacated at the request of the parties because the case was rendered moot by the county's abandonment of the DRE machines at issue. *Stewart v. Blackwell*, 473 F.3d 692, 693 (6th Cir. 2007).

Instead, Plaintiffs "merely speculate and make assumptions about whether their" votes will be inaccurately counted as the result of a potential hack. *Clapper*, 568 U.S. at 411. *See also Stein*, 223 F. Supp. at 432 ("[The p]laintiffs' allegation that voting machines may be 'hackable,' and the seemingly rhetorical question they pose respecting the accuracy of the vote count, simply do not constitute injury-in-fact."). Plaintiffs assert that they "*believe*[] the state's voting system, and in particular its use of iVotronic machines, is deeply unreliable and fundamentally unverifiable" and that they "*believe*[] that these unaddressed flaws impact [their] right to have [their] vote counted accurately." (ECF No. 1 at 5–6 ¶ 12 (emphasis added).) (*See also id.* at 6 ¶ 13 ("[Plaintiff] Leventis has *long-standing concerns* about the accountability, auditability, and transparency of the iVotronic-based system. He reasonably *believes* that the flaws in South Carolina's voting system burden his right to have his vote counted fairly and accurately." (emphasis added)).) The Supreme Court found similar allegations unavailing in *Clapper*. *See* 568 U.S. at 411 ("[Respondents merely speculate and make assumptions about whether their communications with their foreign contacts will be acquired under § 1881a. . . . For example, journalist Christopher Hedges states: 'I have no choice but to *assume* that any of my international communications may be subject to government surveillance, and I have to make decisions . . . in light of that *assumption*.' App. to Pet. for Cert. 366a (emphasis added and deleted). Similarly, attorney Scott McKay asserts that, '[b]ecause of the [FISA Amendments Act], we now have to *assume* that every one of our international communications may be monitored by the government.' *Id.*, at 375a (emphasis added)." (citation omitted)).

Furthermore, Plaintiffs allegations center on the "*vulnerab[ilities*] [of the iVotronic voting machines] to cyberattack[s]." (ECF No. 1 at 2 ¶ 2 (emphasis added).) However, the vulnerabilities of the iVotronic machines to being hacked, in and of themselves, would not cause Plaintiffs' votes

to be inaccurately accounted; someone would still have to hack the machines to alter Plaintiffs' votes. (*See, e.g.*, ECF No. 14 at 17 ("As described at length in the Complaint, the[] [iVotronic] machines have been shown to contain numerous vulnerabilities that *could be exploited by hackers* . . . ." (emphasis added)).) And Plaintiffs can only speculate as to whether "*potential* hackers," (ECF No. 1 at 2 ¶ 3 (emphasis added)), will exploit the vulnerabilities of the iVotronic voting machines,[19] making their allegations "necessarily conjectural." *Clapper*, 568 U.S. at 412. *See also id.* ("Moreover, because § 1881a at most *authorizes*—but does not *mandate* or *direct*—the surveillance that respondents fear, respondents' allegations are necessarily conjectural. Simply put, respondents can only speculate as to how the Attorney General and the Director of National Intelligence will exercise their discretion in determining which communications to target."); *id.* at

[19] Although the Senate Report cited by Plaintiffs does state that "Paperless [DRE] voting machines . . . are at highest risk for security flaws," (ECF No. 1 at 38 ¶ 109 (quoting SSCI, *Russian Targeting of Election Infrastructure During the 2016 Election*)), it also indicates that electronic voting machines were not the target of the Russian affiliated cyber-actors. (*Id.* at 36 ¶ 105 (quoting SSCI, *Russian Targeting of Election Infrastructure During the 2016 Election*).) Rather,

> almost all of the states that were targeted observed vulnerability scanning directed at their Secretary of State websites or voter registration infrastructure. . . . In at least six states, Russian-affiliated cyber actors went beyond scanning and conducted malicious access attempts on voting-related websites. In a small number of states, Russian-affiliated cyber actors were able to gain access to restricted elements of election infrastructure. In a small number of states, these cyber actors were in a position to, at a minimum, alter or delete voter registration data; however, they did not appear to be in a position to manipulate individual votes or aggregate vote totals.

SSCI, *Russian Targeting of Election Infrastructure During the 2016 Election*. Thus, arguably, Plaintiffs can also only speculate as to whether any potential hackers seeking to interfere with an election in South Carolina would do so by hacking the iVotronic voting machines. *Compare with Clapper*, 568 U.S. at 413 ("[E]ven if respondents could demonstrate that the targeting of their foreign contacts is imminent, respondents can only speculate as to whether the Government will seek to use § 1881a-authorized surveillance (*rather than other methods*) to do so." (emphasis added)).

414 ("We decline to abandon our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors.").

Accordingly, as a result of the attenuated chain of inferences on which Plaintiffs' hacking theory of threatened injury rests, Plaintiffs have failed to show their alleged injury is "certainly impending." *See Whitmore*, 495 U.S. at 158 ("Allegations of possible future injury do not satisfy the requirements of Art. III. A threatened injury must be 'certainly impending' to constitute injury in fact." (quoting *Babbitt v. Farm Workers*, 442 U.S. 289, 298 (1979))). Plaintiffs' hacking theory of threatened injury is also too attenuated to satisfy the substantial risk of harm standard. *See Clapper*, 568 U.S. at 414 n.5 ("But to the extent that the 'substantial risk' standard is relevant and is distinct from the 'clearly impending' requirement, *respondents fall short of even that standard, in light of the attenuated chain of inferences necessary to find harm here*." (emphasis added)).[20] *See also Stein*, 223 F. Supp. 3d at 432–33 ("Plaintiffs' allegation that voting machines may be 'hackable,' and the seemingly rhetorical question they pose respecting the accuracy of the vote count, simply do not constitute injury-in-fact. *See, e.g.*, . . . (*Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) (after payroll processor's database was hacked, the plaintiffs' allegations that their personal information could be misused 'rel[ied] on speculation' and did not constitute injury-in-fact).").

[20] "[I]n light of the attenuated chain of inferences necessary to find harm here," *Clapper*, 568 U.S. at 414 n.5, neither do the costs "absorb[ed]" by Plaintiffs to avoid or mitigate the harm they allege support their substantial risk theory. (ECF No. 1 at 5 ¶ 12.) *See Beck*, 848 F.3d at 275 ("Nonetheless, our inquiry on standing is not at an end, for we may also find standing based on a 'substantial risk' that the harm will occur, which in turn may prompt a party to reasonably incur costs to mitigate or avoid that harm." (citing *Clapper*, 568 U.S. at 414 n.5)). *See also Clapper*, 568 U.S. at 416 ("[R]espondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.")

Plaintiffs also fail to show that the alleged threatened injury—the possibility their vote will not be accurately counted due to a hack of South Carolina's voting machines—is traceable to Defendants. *See Clapper*, 568 U.S. at 409 ("To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" (quoting *Monsanto Co.*, 561 U.S. at 149). As Plaintiffs do not allege Defendants would be the "potential" hackers, the potential hackers must be "some third party not before the court." *Lujan*, 504 U.S. at 560 (quoting *Simon*, 426 U.S. at 41–42). (*See also* ECF No. 14 at 17 ("As described at length in the Complaint, the[] [iVotronic] machines have been shown to contain numerous vulnerabilities that *could be exploited by hackers* . . . ." (emphasis added)).) Accordingly, Plaintiffs' hacking theory of injury is not "fairly traceable to the challenged action" of Defendants. *Clapper*, 568 U.S. at 409 (quoting *Monsanto Co.*, 561 U.S at 149). *See also id.* at 414 ("We decline to abandon our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors."); *Doe v. Va. Dep't of State Police*, 713 F.3d 745, 755 (4th Cir. 2013) ("Traceability is established if it is 'likely that the injury was caused by the conduct complained of and not by the independent action of some third party not before the court.'" (quoting *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 154 (4th Cir. 2000))); *Mirant Potomac River, LLC v. EPA*, 577 F.3d 223, 226 (4th Cir. 2009) ("An injury sufficient to meet the causation and redressability elements of the standing inquiry must result from the actions of the respondent, not from the actions of a third party beyond the [c]ourt's control.").

The court next turns to Plaintiffs' standing theory based on the possibility their vote will not be accurately counted due to malfunctions of the iVotronic voting machines. (*See* ECF No. 14 at 23 ("By maintaining a statewide iVotronic system in South Carolina, the [SC]SEC fails to

provide a reliable voting system because it creates a substantial risk that votes will be rendered ineffective, either by intentional wrongdoing or *predictable technological failure*." (emphasis added)).) Here, Plaintiffs' allegations differ from those advanced in connection with its hacking theory because Plaintiffs allege past malfunctions of some of South Carolina's iVotronic voting machines. First, Plaintiffs allege that "the [iVotronic] machines in use in South Carolina have been operating in many instances since 2004, putting them at the end of their life span. As they age, the machines become less reliable and even more susceptible to malicious attack." (ECF No. 1 at 22 ¶ 67.) (*See also id.* at 23 ¶ 69 ("Five years ago, the [2013] LAC Report recognized that iVotronic machines have a lifespan of twelve to fifteen years, and that 'due to [their] age, replacement parts for this system have become problematic and will eventually become obsolete.'" (citing 2013 LAC Report at 2)).) Plaintiffs provide several examples of past machine failures:

> (1) a 2005 election in which machines in Myrtle Beach repeatedly malfunctioned and caused the supply of emergency paper ballots to be "running out"; (2) a 2005 city council primary race in Columbia which initially showed 3,208 total votes, but in which a manual recount revealed only 768 actual votes; and (3) a 2012 Richland County election in which widespread machine breakdowns caused massive delays, leaving voters waiting in line to vote as late as 11:30 p.m. [2013] LAC Report at 13. And in April 2018, twelve voting machines being used in a Goose Creek municipal election broke down with an unresolvable error.

(*Id.* at 22–23 ¶ 68.) In addition to these failures, Plaintiffs allege that

> [i]n the June 2018 primary elections, voting machines malfunctioned across the state, causing lines at the polls and delaying election results. In Greenville County, 33 voting machines at four precincts stopped working. As a result, lines to vote exceeded an hour in at least one Greenville County precinct. This mass mechanical failure delayed the reporting of results and required poll workers to call in an ES&S technician to review the machines' backup storage devices. The ES&S employee, rather than South Carolina poll workers, retrieved votes from the affected machines. Voting machines also broke in Horry, Marlboro, and Florence Counties. Even when the machines did not breakdown entirely, election officials acknowledged that aging touchscreens made it more difficult for voters to make their selections.

(*Id.* at 24–25 ¶¶ 74–75.) Plaintiffs also cite the SCSEC's Fiscal Year 2015-16 Accountability Report, which concludes that "[e]quipment issues and breakdowns are becoming more frequent. As a result, carrying out our mission and reflect[ing] the will of the electorate has become complicated and challenging."[21] (*Id.* at 23 ¶ 70 (quoting SCSEC, FY 2015-16 Accountability Report, at A-6).) The SCSEC's 2016-2017 Accountability Report found that "the [iVotronic] system requires intensive maintenance and enhancements," and stated the SCSEC's "intent to 'continue working with the General Assembly' to secure funding to upgrade and eventually replace the systems."[22] (*Id.* at 23–24 ¶ 71 (citing SCSEC, FY 2016-17 Accountability Report, at A-9).) Plaintiffs note that the SEC's FY 2016-2017 Accountability Report "did not . . . set out a concrete timeline for [upgrading and replacing the system] or acknowledge other avenues that it could undertake of its own to discharge its statutory responsibility, such as financing arrangements with vendors for purchasing or leasing new equipment." (*Id.* at 24 ¶ 71.) Finally, Plaintiffs also allege that "[t]he risk that Plaintiffs' votes will not be accurately counted is also compounded by the absence of any manual recount or audit procedure that could detect interference with the soft-ware provided vote count and provide a subsequent remedy." (ECF No. 14 at 24.)

Though Plaintiffs' malfunction theory presents a closer standing question than their hacking theory, Plaintiffs still fail to show a substantial risk of harm that their votes will not be counted due to potential malfunctions by the iVotronic voting machines. First, Plaintiffs assert they "face similar arbitrary disparities" to those in *Bush v. Gore*, *Black v. McGuffage*, and *Stewart*

[21] South Carolina State Election Commission, *Fiscal Year 2015-16 Accountability Report* (2016), https://www.scvotes.org/files/Acct%20Report%202015-16%20Final.pdf [hereinafter SCSEC, FY 2015-16 Accountability Report].

[22] South Carolina State Election Commission, *Fiscal Year 2016-2017 Accountability Report* (2017) https://www.scvotes.org/sites/default/files/Combined%20document%20-%202017%20Acc%20Report.pdf [hereinafter SCSEC, FY 2016-17 Accountability Report].

v. Blackwell, and cite several other cases as support for their malfunction theory. (*Id.* at 27.) However, all of these cases have significantly distinguishable facts. For example, in *Bush v. Gore*, the United States Supreme Court found that Florida's manual recount policy of "consider[ing] the 'intent of the voter'" lacked "specific standards to ensure its equal application." 531 U.S. 98, 105–06 (2000). The lack of such standards, the Supreme Court found, "led to unequal evaluation in ballots . . . . [and] the standards for accepting or rejecting contested ballots might vary not only from county to county but indeed within a single county from one recount team to another." *Id.* at 106. Furthermore, in *Bush*, there were specific counties at issue and identifiable numbers of, for example, overvotes. *See id.* at 100 ("On December 8, 2000, the Supreme Court of Florida ordered that the Circuit Court of Leon County tabulate by hand 9,000 ballots in Miami–Dade County. It also ordered the inclusion in the certified vote totals of 215 votes identified in Palm Beach County and 168 votes identified in Miami–Dade County for Vice President Albert Gore, Jr., and Senator Joseph Lieberman, Democratic candidates for President and Vice President. . . . The court further held that relief would require manual recounts in all Florida counties where so-called 'undervotes' had not been subject to manual tabulation."). Thus, not only was there unequal treatment of votes depending on the county where a Florida voter cast their vote, there was also evidence that there were over 100,000 overvotes. *See id.* at 108. As Plaintiffs do not allege different methods of tabulating votes that advantage certain candidates and voters over others, or identify any number of vote discrepancies, the disparities they allege differ substantially from those in *Bush*.[23]

[23] "The Supreme Court explicitly warned that *Bush,* if not entirely a one-day ticket, was decided on extraordinary facts, such that its holding 'is limited to the present circumstances.'" *Green Party of State of N.Y. v. Weiner*, 216 F. Supp. 2d 176, 192 (S.D.N.Y. 2002) (quoting *Bush*, 531 U.S. at 109).

The same is true of the other cases cited by Plaintiffs. In these cases, either the plaintiffs voted in counties that used a less reliable voting system compared to those in use by other counties in the state; the plaintiffs were unable to vote—literally disenfranchised; the plaintiffs had to wait a substantial amount of time to vote; or the voting system disproportionately affected voters of certain races or nationalities. The court quotes from these decisions at length to highlight the factual differences between Plaintiffs' allegations and the allegations in the cases relied on by Plaintiffs. *See, e.g.*, *Arcia v. Fla. Sec'y of State*, 772 F.3d 1335, 1341 (11th Cir. 2014) (finding the plaintiffs had standing to sue "because they were directly injured by [the Florida Secretary of State's program to remove suspected non-citizens from the voter rolls within ninety days of a federal election] when they were wrongly identified as non-citizens"); *League of Women Voters of Ohio v. Brunner*, 548 F.3d 463, 466–67 (6th Cir. 2008) (finding plaintiffs had standing to challenge the touchscreen voting machines used in Ohio when their complaint alleged, among other things, that some registered Ohio voters were denied the right to vote and had to wait several hours, in one case nine (9), to vote due to a polling place having only one voting machine after one broke down); *Stewart*, 444 F.3d at 846, 847–48, 861 (finding African-American and Caucasian voters residing in four Ohio counties had standing to challenge the use of punch-card ballots in the counties where they cast their votes because other counties in Ohio utilized more reliable voting methods and the plaintiffs submitted a report that found thousands of Ohio voters had been disenfranchised by antiquated voting equipment); *Curling*, 334 F. Supp. 3d 1303, 1314–15 (N.D. Ga. 2018) (finding the plaintiffs had standing to challenge the use of DRE voting machines when they alleged that Georgia's DRE voting system had been hacked multiple times and, in at least one instance, a voter was unable to vote due to a software glitch that removed his name from the

eligible voter rolls);[24] *Mich. State A. Philip Randolph Inst. v. Johnson*, 209 F. Supp. 3d 935, 944 (E.D. Mich. 2016) (finding the plaintiffs had standing and had not alleged a general grievance applicable to every voter in the state because the plaintiffs "allege[d] that [the challenged legislation] will disproportionately impact African-Americans in urban areas in the form of longer wait times"); *Black v. McGuffage*, 209 F. Supp. 2d 889, 892, 894 (N.D. Ill. 2002) (finding plaintiffs had standing based on their allegations that of the four available voting systems available in Illinois, "jurisdictions that employ[ed] either punch-card voting systems or provide optical scan without error notification experience a higher percentage of residual votes than those jurisdictions that use optical scanning equipment with error notification (a residual vote is a ballot that does not contain a permissible vote)"; "individuals living in punch card jurisdictions have a greater statistical probability of not having their votes counted"; and "the counties with the punch-card system have larger populations of minorities than do counties using other voting systems, and thus use of those less accurate machines has a disparate impact on minority voters"); *Common Cause S. Christian Leadership Conference of Greater L.A. v. Jones*, 213 F. Supp. 2d 1106, 1107–08 (C.D. Cal. 2001) (denying the defendant's motion for judgment on the pleadings because the plaintiffs alleged that "punch card voting systems are less reliable than the other voting systems permitted by the secretary of state," "individuals living in counties where the punch-card system is used are

[24] The plaintiffs in *Curling* also made allegations similar to those made by Plaintiffs:

> Donna Price 'cast her vote on a DRE in the 2016 General Election,' and '[w]ithout the intervention of this [c]ourt, Price will be compelled to choose between relinquishing her right to vote and acquiescing to cast her vote under a system that violates her right to vote in absolute secrecy and have her vote accurately counted'. . . 'DREs produce neither a paper trail nor any other means by which the records of votes cast can be audited.' [Curling Complaint, Doc. 70 ¶ 16].

334 F. Supp. 3d at 1315. However, these allegations did not stand alone; they were accompanied by allegations of *actual* hacking and disenfranchisement. *See id.* at 1314–15 (emphasis added).

substantially less likely to have their votes counted," and "the counties which choose the punch-card system have high racial minority populations in comparison with counties using other voting systems").

The court has identified some cases that better mirror Plaintiffs' claims. In these cases, the courts found the plaintiffs did not have standing. For example, in *Stein v. Cortes*, 2016 Presidential Candidate Jill Stein and Pennsylvania voter Randall Reitz sought a recount of Pennsylvania's votes for President of the United States based on their claim that "[DRE] machines might be vulnerable to hacking and cyberattacks."[25] 223 F. Supp. 3d 423, 427 (E.D. Pa. 2016). More specifically, Plaintiffs Stein and Reitz alleged that "Pennsylvania's DRE machines are 'vulnerable, hackable, [and] antiquated,' that the Pennsylvania Election Code's recount provisions are 'labyrinthine, incomprehensible, and impossibly burdensome,' and that neither Dr. Stein nor her voters have been permitted to examine the machines. (*See* Compl. ¶¶ 1–5, 63, 82, Doc. No. 1.)." *Id.* at 432. The court found it "significant" that the plaintiffs did not "question whether Pennsylvania votes were correctly counted," and "ma[de] no factual allegations respecting Mr. Reitz other than that he 'is a voter in the State of Pennsylvania, and voted in the 2016 presidential election.' ([Compl.] ¶ 10.)." *Id.* Ultimately, the court found "[t]hese allegations insufficient to confer standing" because (1) Plaintiff Reitz did not allege that "his vote was inaccurately recorded or tallied in the final Pennsylvania vote count"; (2) the plaintiffs' "allegation that voting machines may be

[25] During the November 8, 2016 Presidential election,

> the Commonwealth allowed its citizens to cast votes on Direct Recording Electronic (DRE) machines, and used optical-scan machines to tabulate paper ballots. Fifty-four Pennsylvania Counties used one of six DRE machine models. Seventeen Counties used paper ballots that were then counted using optical-scan machines. Four Counties used both DRE and optical-scan machines.

Stein, 223 F. Supp. 3d at 427 (citation omitted).

'hackable,' and the seemingly rhetorical question they pose respecting the accuracy of the vote count, simply do not constitute injury-in-fact"; and (3) the plaintiffs sought "to protect the rights of all Pennsylvania voters," meaning the plaintiffs' alleged injury was not personal to them. *Id.* at 432–34. The United States District Court for the Eastern District of Pennsylvania reached the same conclusion in *Landes v. Tartaglione*, a similar case in which the plaintiff alleged "electronic voting machines" were vulnerable to both hacking and technical failure. No. CIV.A. 04-3163, 2004 WL 2415074, at *3 (E.D. Pa. Oct. 28, 2004) ("[The plaintiff] alleges only a 'conjectural or hypothetical' injury. She argues that voting machines are vulnerable to manipulation or technical failure, but she does not assert that the voting machines in question have actually suffered from these issues in the past or that they will definitively malfunction or be tampered with during the upcoming election."); *see id.* ("[The] plaintiff's allegations here are not sufficient to demonstrate injury in fact because they are conjectural. If plaintiff's vote and the votes of all other voters in the upcoming election are correctly recorded, plaintiff will suffer no injury. Plaintiff's reliance on the terms 'if' and 'may' to couch her allegations of harm is a clear indication that the harm she alleges is merely speculative.").

Also, the United States District Court for the Northern District of New York came to the same conclusion in *Schulz v. Keller*, in which the plaintiffs alleged that "the machine error and human fraud resulting from [the d]efendants' voting procedures" during the 2008 elections "violated their voting rights, contract rights, and constitutional rights." 2011 WL 2669456, at *1, *7. First, the court noted that "[t]he Second Circuit has joined other circuits in holding that 'a voter fails to present an injury-in-fact when the alleged harm is abstract and widely shared.'" *Id.* at *6 (quoting *Crist v. Comm'n on Presidential Debates*, 262 F.3d 193, 195 (2d Cir. 2001)). The court found that because the plaintiffs' alleged injury based on the "inevitability of machine error"

and "human fraud" was "widely shared by all voters in the state of New York, it is an abstract one and as such cannot constitute an injury in fact." *Id.* The court further concluded that

> [E]ven construing their Amended Complaint to mean that the machine error and human fraud resulting from [the d]efendants' voting procedures will also harm [the p]laintiffs—whose votes will allegedly not be counted accurately—the [c]ourt finds that these allegations are merely conjectural and hypothetical and do not demonstrate a concrete or particularized injury to [the p]laintiffs. [The p]laintiffs have not presented any concrete or specific factual allegations from which the [c]ourt could infer, for instance, that their votes were diluted, that they are being disfavored by a gerrymandering scheme, or that they were unfairly denied access to a polling station.

Id. at *7.

This court acknowledges that Plaintiffs' allegations are more extensive, and better supported by, for example, expert reports, than the plaintiffs in *Stein*,[26] *Landes*, and *Schulz*. And, Plaintiffs do allege that the iVotronic machines have malfunctioned on several occasions and are approaching end of life. (*See* ECF No.1 at 22–23 ¶ 68; 24–25 ¶ 74). For example, Plaintiffs allege that "[]n Greenville County 33 voting machines at four precincts stopped working. As a result, lines to vote exceeded an hour in at least one Greenville County precinct." (ECF No. 1 at 24–25 ¶ 74.) Plaintiffs describe this as a "mass mechanical failure."[27] (*Id.* at 25 ¶ 74.) Similarly,

[26] The *Stein* plaintiffs did submit the reports of four experts who found Pennsylvania's DRE machines were vulnerable to hacking and tampering. *Stein*, 223 F. Supp. 3d at 441. However, the judge found that "[e]ven if I were to credit these opinions, they make out little more than the theoretical possibility a voting machine somewhere in the Commonwealth might be susceptible to tampering." *Id.*

[27] There are twenty-nine (29) voting precincts in Greenville, South Carolina. *South Carolina Precinct Information Greenville County*, South Carolina Election Commission, https://www.scvotes.org/cgi-bin/scsec/precinctnew?countykey=GREENVILLE (last visited Feb. 1, 2019). *See also White Tail Park, Inc.*, 413 F.3d at 459 (" When a defendant raises standing as the basis for a motion under Rule 12(b)(1) to dismiss for lack of subject matter jurisdiction, . . . the district court 'may consider evidence outside the pleadings without converting the proceeding to one for summary judgment.'" (quoting *Richmond, Fredericksburg & Potomac R.R. Co.*, 945 F.2d at 768)).

Plaintiffs allege that "in April 2018, *twelve* voting machines being used in a Goose Creek municipal election broke down with an unresolvable error." (*Id.* at 23 ¶ 68.) However, allegations such as these show only that at some precincts in some counties in South Carolina, some of the iVotronic machines have malfunctioned, which, given the nature of machines, is to be expected. *See Nat'l Ass'n for Advancement of Colored People (NAACP) State Conference of Pa. v. Cortes*, 591 F. Supp. 2d 757, 765 (E.D. Pa. 2008) ("The evidence, not surprisingly, demonstrated that DRE voting machines, like all other machines, sometimes fail.").[28] *Cf. Stein*, 223 F. Supp. 3d at 441 (stating in response to expert reports that Pennsylvania's DRE machines were vulnerable to hacking and tampering that "[e]ven if I were to credit these opinions, they make out little more than the theoretical possibility a voting machine somewhere in the Commonwealth might be susceptible to tampering."). Plaintiffs' allegations do not show that a majority, or even a large number, of the iVotronic voting machines in a majority, or even a large number, of counties in South Carolina malfunction during elections. *Cf. NAACP Conference of Pa.*, 591 F. Supp. 2d at 765 ("Based on the record before us, we find that there is a real danger that a *significant* number of machines will malfunction throughout the Commonwealth, and this occurrence is likely to cause unacceptably long lines on November 4 . . . ." (emphasis added)). Moreover, in the 2013 LAC Report cited by Plaintiffs, the LAC found the reported errors with the iVotronic machines were

[28] *See NAACP State Conference of Pa.*, 591 F. Supp. 2d at 764 ("It cannot be denied that the malfunctioning of DRE voting machines, either because of human error or mechanical failure, causes a significant injury *whenever voters are effectively denied the right to cast their ballots*. Some waiting in line, of course, is inevitable and must be expected. Citizens have to sign in at the polling place and wait their turn to retire behind the curtain to cast their votes. One must always choose between and among a number of candidates for different offices listed on the ballot and often, as in this election, there are questions to be read and considered. All of this takes time. Nonetheless, there can come a point when the burden of standing in a queue ceases to be an inconvenience or annoyance and becomes a constitutional violation because it, in effect, denies a person the right to exercise his or her franchise. There is no bright line or 'litmus-paper test.' As *Anderson[v. Celebrezze*, 460 U.S. 780 (1983)] teaches, we must consider all the relevant factors."

"largely categorized as human errors rather than mechanical errors," which undermines Plaintiffs' allegations that the iVotronic machines are so inherently error-prone that their certification by Defendants creates a substantial risk that Plaintiffs' votes will not be accurately counted. 2013 LAC Report at 13.

Furthermore, numerous times throughout their pleadings, Plaintiffs assert that their alleged injury—the possibility their vote will not be accurately counted due to the malfunctioning or hacking of South Carolina's iVotronic voting machines—is shared by "all South Carolina voters." (*See e.g.*, ECF No. 14 at 7 ("Plaintiffs Frank Heindel and Phil Leventis are South Carolina voters who seek to ensure that their ballots, *and the ballots of all South Carolina voters*, are counted fairly and accurately. They filed this lawsuit because Defendants, in their capacities administering the [SCSEC] have failed to provide *South Carolina voters* with an election system that lives up to that basic expectation." (emphasis added)); *id.* at 25 ("The flawed system also subjects Plaintiffs, and *all South Carolina voters*, to a systemic risk of arbitrary disparities in the effectiveness of their ballots." (emphasis added)); *id.* at 28 ("Plaintiffs, *like all South Carolina voters*, have no way to assess in advance whether their county or precinct faces a particularly elevated threat in any given election." (emphasis added)). Therefore, as Plaintiffs' allegations are not personal to Plaintiffs, and could be advanced by any South Carolina voter, Plaintiffs' "asserted harm is a 'generalized grievance' shared in substantially equal measure by all or a large class of citizens." *Warth v. Seldin*, 422 U.S. at 499. *See also Spokeo, Inc.*, 136 S. Ct. at 1548 n.7 ("The fact that an injury may be suffered by a large number of people does not of itself make that injury a nonjusticiable generalized grievance [as long as] *each individual suffers a particularized harm*." (emphasis added)); *Landes*, 2004 WL 2415074, at *3 (finding the plaintiff's allegations that "the use of voting machines deprives her of her rights to vote, to have votes counted properly, to observe the voting

process effectively and to have those rights fully enforced" and "she has been injured in past elections and will be injured in this election because voting machines prevent her from observing whether or not her vote has actually been cast" amounted to a generalized grievance). *Cf. Black*, 209 F. Supp. 2d at 894–95 ("[The d]efendants argue that [the p]laintiffs have asserted a generalized grievance and that the statistical likelihood of future injury is insufficient to bring standing. [The p]laintiffs allege that African American and Latino voters suffered injury when they use the challenged voting systems because they voted in the 2000 election in precincts recording a substantial and disproportionate number of undervotes. As the district court held in *Andrews v. Cox*, No. 1:01–CV–319–ODE (N.D. Ga. Aug. 20, 2001), '[the] plaintiffs sufficiently allege a personal injury. . . by the disproportionate risk of having their votes not counted.' Slip op. at 8. The ballot machinery used in the jurisdictions in which [the p]laintiffs vote increases the likelihood that their votes will not be counted."). And, "the [c]ourt has refrained from adjudicating 'abstract questions of wide public significance' which amount to 'generalized grievances,' pervasively shared and most appropriately addressed in the representative branches." *Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc.*, 454 U.S. 464, 475 (1982) (quoting *Warth*, 422 U.S. at 499–500).

There is substantial space between elections administered perfectly and elections administered in a way that unconstitutionally burdens the right to vote. This space is the domain of the states, where "[t]he law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches." *Clapper*, 568 U.S. at 408. *See also* U.S. Const. Art. I, § 4, Cl. 1 (authorizing the states to regulate the "Times, Places and Manner of holding elections for Senators and Representatives"); *Lassiter v. Northampton Cty. Bd. of Elections*, 360 U.S. 45, 50 (1959) ("The

States have long been held to have broad powers to determine the conditions under which the right of suffrage may be exercised, absent of course the discrimination which the Constitution condemns." (citations omitted)). Plaintiffs' allegations, though they may show that there is *some* conceivable risk that Plaintiffs' votes will be inaccurately counted, fall within this space, and are, therefore, insufficient to confer standing. *See Susan B. Anthony*, 573 U.S. at 158 ("'An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a '"substantial risk" that the harm will occur.'" (quoting *Clapper*, 568 U.S. at 414 n.5)); *Food & Water Watch, Inc. v. Vilsack*, 79 F. Supp. 3d 174, 189 (D.D.C) ("But a plaintiff who plans to satisfy the imminent injury requirement by alleging that the challenged act will increase the risk of harm to her, must do more than merely assert that there is some conceivable risk that she will be harmed on account of the defendant's actions.").

IV. CONCLUSION

The court finds Plaintiffs' allegations are insufficient to confer standing. Therefore, the court (1) **GRANTS** Defendants' Motion to Dismiss under Rule 12(b)(1) of the Federal Rules of Civil Procedure (ECF No. 5 at 1); (2) **DISMISSES** Plaintiffs' Complaint (ECF No. 1) without prejudice;[29] (3) **DENIES** Defendants' Motion to Dismiss under Rule 12(b)(6) of the Federal Rules of Civil Procedure as moot (ECF No. 5 at 1); and (4) considers Defendants' Motion for Summary Judgment (ECF No. 5) to be withdrawn based on Defendants' representation at the hearing on these motions (ECF No. 49 at 13:14–18).

IT IS SO ORDERED.

[29] "A dismissal for lack of standing—or any other defect in subject matter jurisdiction—must be one without prejudice, because a court that lacks jurisdiction has no power to adjudicate and dispose of a claim on the merits." *S. Walk at Broadlands Homeowner's Ass'n, Inc. v. OpenBand at Broadlands,* LLC, 713 F.3d 175, 185 (4th Cir. 2013).

United States District Judge

February 8, 2019
Columbia, South Carolina