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; and MARK A. BENSON, MARILYN BOWERS, and NICOLE SPAIN WHITE, Members of the South Carolina State Election Commission, in their official capacity, Defendants.	)	Civil Action No.

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

PRELIMINARY STATEMENT

1. The right to vote is the cornerstone of our democratic system of government, a fundamental guarantee that preserves all other rights. The right to vote depends on a system of election administration that provides all eligible voters with an effective opportunity to participate. At an irreducible minimum, this means ensuring that the machinery of democracy has the capacity to record and count each vote consistently, fairly, effectively, and accurately. The reliability of that basic element of democracy is under extraordinary stress across the country as election systems face threats posed by hackers, who may seek to gain

unauthorized access to data or computer systems to mount cyberattacks aimed at manipulating, damaging, or destroying those systems. The problem is especially acute in South Carolina.

2. In South Carolina, the capacity of the state's election system to record and count votes reliably is deeply compromised by the state's unnecessarily vulnerable voting system. Throughout the state, elections are administered using a voting system—the iVotronic Direct Recording Electronic ("DRE") system, manufactured by Election Systems & Software ("ES&S")—that computer science experts have shown to be highly vulnerable to cyberattack and malware infections, which can occur whether or not the machine is directly connected to the internet.

3. Over a decade ago, respected security researchers and computer science scholars studied the iVotronic and demonstrated that its system presented potential hackers with numerous pathways to attack. Flaws in the iVotronic's hardware (the machines themselves) and software (the programs running on the machines) create the kind of vulnerability that sophisticated hackers could not only exploit, but exploit in a manner that would cause widespread disruption. As one team of researchers studying the iVotronic found in 2007, "[i]nserting malicious code at any step in this process could result in a virus spreading to all other components, completely compromising the election." In other words, the iVotronic machines used in South Carolina are so vulnerable that a cyberattack against one machine could result in precinct-wide—or even county-wide—malfunction.

4. These vulnerabilities are especially critical because the iVotronic machines used in South Carolina are entirely digital. They produce no record of voter intent apart from the data contained within the system. In the event of a suspected cyberattack—or even a

malfunction—the only reference points against which to check the ostensible election results are other components of that same potentially compromised computer system. This makes meaningful audit and recount procedures impossible. A successful cyberattack could unfold consistently across parts or all of the iVotronic system, from a single machine to the tallying of vote totals across counties, leaving no way to identify the damage. South Carolina is one of only five states in the country in which electronic voting machines that produce no paper record of voter intent are used statewide.

5. Because the iVotronic system is used statewide, its vulnerabilities impair the reliability of elections in every precinct and county. Those inherent vulnerabilities are exacerbated by the varying cybersecurity practices employed in each county. As a result, a hacker might cause largescale disruption by attacking one or more counties, potentially creating distrust and confusion that could affect the entire state.

6. The risks inherent in the state's election system have become only more acute in recent years, as demonstrated by numerous widely acknowledged attacks on election infrastructure starting in 2016. Against the backdrop of a surging set of cyber-threats designed to disrupt and undermine confidence in the democratic process, including documented attacks by foreign nation-states and a history of inadequate cyber safeguards in South Carolina, these vulnerabilities implicate the Plaintiffs' fundamental constitutional right to vote.

7. Plaintiffs Frank Heindel and Phil Leventis are South Carolina voters seeking to vindicate their right to participate effectively in the state's elections. They are registered voters who regularly vote in person on iVotronic machines. Mr. Heindel, a commodities trader who has lived in Charleston County for over 20 years, has spent the last decade

investigating security flaws in South Carolina's voting system, including drafting a 2010 report on unexplained inconsistencies in iVotronic election results certified in several South Carolina counties. Mr. Leventis served eight terms in the South Carolina Senate, including during the time the State Election Commission ("SEC") adopted the current iVotronic-based system, which he opposed. Security flaws in South Carolina's voting system harm the Plaintiffs' right to participate in South Carolina elections and to have their votes counted accurately.

8. Defendants are the Executive Director, Chair, and Members of the SEC. They are responsible for administering the state's election system in compliance with the law. They have been on notice for over a decade about these severe vulnerabilities and have failed to resolve them.

9. By failing to provide South Carolina voters with a system that can record their votes reliably, Defendants deprive Plaintiffs of their fundamental right to vote, in violation of the U.S. Constitution. "Obviously included within the right to choose, secured by the Constitution, is the right of qualified voters within a state to cast their ballots and have them counted. . . ." *United States v. Classic*, 313 U.S. 299, 315 (1941). And as the Supreme Court has long understood, "the right of suffrage can be denied by a debasement or dilution of the weight of a citizen's vote just as effectively as by wholly prohibiting the free exercise of the franchise." *Reynolds v. Sims*, 377 U.S. 533, 555 (1964). South Carolina's vulnerable election infrastructure is not a sufficiently reliable system to meet the constitutional standard.

10. Defendants have acknowledged that the state's voting system is not sustainable. They have recognized that it is composed of antiquated machines approaching or exceeding their anticipated lifespan. They also have acknowledged that the current system lacks a

durable and verifiable record of voter intent (*i.e.*, a paper ballot) that would permit verification of whether election results reflect the actual decisions made by South Carolina voters. Defendants have gestured toward a future in which the SEC replaces the existing inadequate iVotronic machines with machines that will be less vulnerable to cyberattack. Yet even as they have articulated that message for years, they have nonetheless maintained a voting system whose fundamental unreliability impermissibly burdens Plaintiffs' right to vote.

11. Defendants are obligated by law to select effective election systems—and to change course when existing systems fall short of constitutional and statutory requirements. This lawsuit seeks to ensure that Defendants discharge those duties to fortify the state's election systems against attack. The Constitution does not require Defendants to ensure perfectly error-free elections or impenetrable cyber-defenses. It does, however, require them to put in place meaningful safeguards against known threats and maintain an election system that provides Plaintiffs with a reasonably reliable assurance that their votes will be counted.

PARTIES

12. Plaintiff Frank Heindel is a resident of Mt. Pleasant, South Carolina, and a registered voter in Charleston County, South Carolina. Mr. Heindel votes regularly, and typically does so in person at his polling place on an iVotronic machine. Mr. Heindel plans to vote in person at his polling place in the November 2018 election. Over the last decade, Mr. Heindel has devoted considerable time and money toward trying to identify and correct the serious security flaws in South Carolina's voting system, including by filing and negotiating numerous state FOIA requests and by conducting an audit of the certified results in South Carolina's November 2010 elections. He felt compelled to absorb these costs

because he believes the state's voting system, and in particular its use of iVotronic machines, is deeply unreliable and fundamentally unverifiable. Mr. Heindel reasonably believes that these unaddressed flaws impact his right to have his vote counted accurately.

13. Plaintiff Phil P. Leventis is a former eight-term South Carolina state senator and a resident of Sumter County, South Carolina. Mr. Leventis is registered to vote in South Carolina, and generally votes in person at his polling place on an iVotronic machine. On the occasions when he votes absentee, he typically does so in person on an iVotronic machine. Mr. Leventis plans to vote in person at his polling place in the November 2018 election. Based on his experiences as a state senator and South Carolina voter, Mr. 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.

14. Defendant Marci Andino is the Executive Director of the South Carolina State Election Commission. She has held that position since 2003. As Executive Director, Defendant Andino is responsible for purchasing, leasing, or contracting for equipment to be used in South Carolina elections. Defendant Andino is sued in her official capacity.

15. Defendant Billy Way, Jr., is the Chair of the South Carolina State Election Commission. The State Election Commission is responsible for approving and adopting the voting system or systems used in South Carolina elections, and for supporting local authorities in the use of that system. Defendant Way is sued in his official capacity.

16. Defendant Mark A. Benson is a member of the South Carolina State Election Commission. Defendant Benson is sued in his official capacity.

17. Defendant Marilyn Bowers is a member of the South Carolina State Election Commission. Defendant Bowers is sued in her official capacity.

18. Defendant Nicole Spain White is a member of the South Carolina State Election Commission. Defendant White is sued in her official capacity.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because the claims in this action arise under federal law, specifically 42 U.S.C. § 1983 and the Fourteenth Amendment to the U.S. Constitution.

20. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because all Defendants are domiciled in South Carolina, and a substantial portion of the events giving rise to this litigation took place there.

FACTUAL ALLEGATIONS

The Architecture of South Carolina's Electronic Voting System

21. All polling places in South Carolina use the iVotronic version 9.1.6.2 voting system, which is manufactured by ES&S. The iVotronic machines are DRE terminals, meaning that a voter enters her choices by selecting options shown on a touchscreen, and the machine ostensibly records her selections in an electronic file that poll workers download after the close of voting. Although some iVotronic machines used in other states also produce a paper record reflecting the voter's selections for the voter to review and verify, the machines used throughout South Carolina do not.

22. South Carolina's procurement of the iVotronic system originated in a Request for Proposals published by the SEC in 2003. After a contentious bidding process, the SEC awarded the contract to ES&S in August 2004.

23. Between 2004 and 2006, the SEC purchased iVotronic machines and related components and software, including over 11,000 touchscreen machines, for approximately $35,000,000. South Carolina deployed the first wave of iVotronic machines in 19 counties in November 2004, and the machines appeared statewide in 2006.

24. 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 each from each machine.

This hardware appears in Diagrams 1 and 2

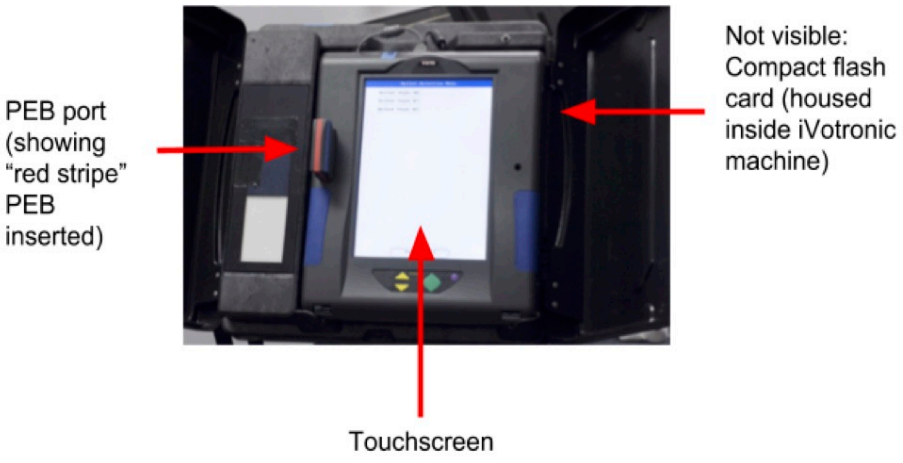

Diagram 1.

"Red stripe" PEB

Diagram 2.

25. 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 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 SEC certified in August 2006.

26. 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 SEC's server systems to translate the data captured via the iVotronic firmware into election results by county as well as statewide.

27. 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.

28. 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,[1] 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.

29. 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.

30. 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.

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

[1] We use the term "voter terminal" and "voting machine" interchangeably to refer to the touchscreen-equipped devices used by individual voters to cast their ballots.

The Role of Poll Managers in Operating South Carolina's Electronic Voting System

32. The SEC hires poll managers to staff polling places on Election Day. The SEC's published materials do not contain any vetting procedures governing who may serve as a poll manager. Poll managers need only be registered voters in the relevant county, or in a county adjoining that county. SC Code. § 7-13-110. Poll managers complete training and take an oath. SC Code § 7-13-72. On Election Day, several poll managers may serve at each precinct.

33. The security of the iVotronic system at any polling place on Election Day is entrusted to poll managers. For example, the SEC's Poll Managers Handbook instructs poll managers to "Make sure PEBs are secured in the communications pack when not in use. When PEBs are in use make sure they are not left unattended." South Carolina Election Commission, "Poll Managers Handbook," (updated April 2018), at 5.[2]

34. On information and belief, however, poll managers often leave PEBs unattended as they carry out their many duties in managing polling sites.

35. Poll managers use PEBs to prepare each machine in a precinct for use that day, and then to enable each voter to cast her ballot. At the beginning of Election Day, the poll manager uses the master PEB to load the election information onto each iVotronic DRE machine and open it for voting. The poll manager also uses the master PEB to print a "zero tape" from a supervisor terminal—a distinct terminal much like those used by voters, but instead used by poll workers to manage various processes over the course of the election. The zero tape ostensibly shows that zero votes have been cast that day. The Poll Managers

[2] Available online at https://www.scvotes.org/sites/default/files/SEC%20MNL%201100-201804%20Poll%20Managers%20Handbook.pdf.

Handbook acknowledges that a supervisor terminal may fail to print a zero tape or may reflect that votes already appear in the data stored on the machine. But the Handbook contains no explanation of why such an event might occur or what a poll worker is to do if it does. Rather, the Handbook instructs poll workers to proceed with voting and notify the county clerk, who is to send a technician to look at the machine. If workers are able to open the machines and print the zero tape, the Handbook directs them to store the master PEB, which will eventually be used to transmit election results back to county headquarters, in an undefined "secure area."

36. When voting is underway, poll workers escort each voter to a terminal, insert a voter PEB into the terminal, and select the appropriate ballot for the voter, as determined by his address. The voter then follows the machine's prompts to enter his votes.

37. After voting concludes, the poll manager takes the master PEB to each machine and prompts the machine to close. Before the machine closes, the master PEB uploads data meant to show that machine's vote totals. The poll manager then inserts the master PEB into the supervisor terminal, which generates a tape stating the precinct's vote tally, as reflected on the machines. At that point, poll workers take the master PEBs to headquarters to be uploaded into the county's election management system. The poll manager also removes the compact flash card from each voting terminal and sends it to county headquarters.

South Carolina Uses an Inherently Unsafe Voting System that Experts Have Shown—Repeatedly—to Be Vulnerable to Hacking

38. The iVotronic system is plagued with vulnerabilities that undermine its reliability and open numerous pathways for potential hacking. For over a decade, computer science experts have sounded repeated alarms over the iVotronic's security flaws.

39. For example, in 2007, Ohio's Secretary of State commissioned several leading computer security and computer science experts to analyze the security of the voting systems used in that state, including the iVotronic. The report that those researchers produced, "EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing" ("EVEREST Report"), offers a rigorous assessment of the security features—and vulnerabilities—of several voting systems. It is especially critical of the iVotronic system. The report became public in December 2007. (Excerpts from the EVEREST Report are attached hereto as Exhibit 3.)

40. The EVEREST researchers 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." EVEREST Report at 29.

41. Grouping these weaknesses into categories—or "four fundamental, pervasive deficiencies"—the EVEREST researchers pointed to: (i) "Ineffective access control"; (ii) "Critical errors in input processing"; (iii) "Ineffective protection of firmware and software"; and (iv) "Ineffective cryptography and data authentication." *Id.* at 49.

42. "Ineffective access control" refers to the exposure of the iVotronic's hardware to tampering or intrusion when deployed at election sites. *See, e.g.*, *id.* at 49-53. As the EVEREST researchers found, "[a]ccess to the iVotronic DRE configuration is protected by several hardware and password mechanisms, all of which can be defeated through apparently routine poll worker (and in some cases voter) access." *Id.* at 50. For example, each

iVotronic machine features a PEB port on the face of the machine, allowing a poll worker or voter—or anyone with access to the machine—to use a PEB to make changes to data stored on the iVotronic. While some functions have an additional layer of password protections, those password protections can be overcome by using a tampered-with or forged PEB. Such PEBs are "easily forged using inexpensive commodity devices such as palmtop computers." *Id.* at 29. In other words, a hacker with a decade-old Palm Pilot (or another device with an infrared connection mechanism) could bypass passwords meant to secure the machines.

43. "Critical errors in input processing" refers to exploitable errors in the software running throughout the iVotronic system. According to the EVEREST experts, a "root cause of the security and reliability issues present in the system is the visible lack of sound software and security engineering practices. Examples of poor or unsafe coding practices, unclear or undefined security goals, technology misuse, and poor maintenance are pervasive. This general lack of quality leads to a buggy, unstable, and exploitable system." *Id.* at 29.

44. In the iVotronic machine, this includes numerous "buffer overflow software bugs," which allow a virus to enter the system at a precinct and then wreak havoc back at headquarters. Someone who exploits any of the system's numerous vulnerabilities in order to input data on the system—for example, by loading malicious code onto an iVotronic PEB or counterfeit PEB—"can exercise complete control over the results reported by the entire county election system." *Id.* at 53. The EVEREST researchers successfully carried out an attack along these lines in their research lab. *See id.* at 53-54.

45. "Ineffective protection of firmware and software" refers to vulnerabilities that would allow a hacker to alter or replace the software or firmware running throughout the system. "The consequences of any attack that alters, replaces or otherwise compromises

[the] software or firmware are sweeping and often impossible to recover from." *Id.* at 54. The EVEREST researchers "found exploitable vulnerabilities that allow an attacker to replace or alter the firmware and software of virtually every component of the ES&S system, either by circumventing access controls or by triggering software errors." *Id.*

46. "Ineffective cryptography and data authentication" refers to the iVotronic's failure to safeguard the system's component pieces—and especially the removable hardware, like flash drives and PEBs, which pass through many hands on Election Day—against unauthorized use. Typically, the way to provide adequate security to such a system is to use robust cryptographic techniques. According to the EVEREST researchers, however, "[t]he iVotronic DRE system does use cryptography, but errors in its implementation render the protection completely ineffective." *Id.* at 57. For example, most data on iVotronic PEBs is encrypted—but the cryptographic key is stored on the same device in unencrypted form. *Id.* at 57-58.

47. Each of these four security failures in the iVotronic is itself a critical vulnerability. The cumulative effect of the deficiencies in the system's many components places the iVotronic at especially high risk of compromise. The EVEREST Report concluded that "systemic weaknesses throughout the system's overall design and implementation . . . render the system as a whole especially difficult to secure in practice." *Id.* at 49.

48. While some means by which a hacker could access the iVotronic system may be mitigated through procedural safeguards, the EVEREST researchers concluded that "taken as a whole, the security failures in the ES&S system are of such magnitude and depth that . . . procedural change alone [is] unlikely to meaningfully improve security." *Id.* at 30.

49. Vulnerabilities diagnosed by the EVEREST researchers present attackers with pathways to large-scale tampering with elections. As the report found, "there is a strong potential for practical attacks that propagate 'virally' from the field back to the county election management system." *Id.* at 49.

50. The architecture of the iVotronic system creates numerous inroads for potential hackers. The fact that machines are not connected to the internet does not insulate the system from attacks. For example, the PEBs used to open and close the voting machines and collect votes are actually small computers that interact with each iVotronic machine, and are fully capable of transferring a virus to the machine. An infected machine can then transfer the virus to another—previously clean—PEB, on which the virus can travel to other machines and back to county election headquarters. Stated differently, PEB devices act as viral hosts. If one malicious PEB infects a single iVotronic machine with a software virus, that virus can propagate through PEB devices later connected with the infected machine to infect other voting machines and, eventually, the central server used at county headquarters, with widespread—and potentially undetectable—consequences for the entire county's election process. *See, e.g., id.* at 57.

51. Infecting a legitimate PEB device is not even necessary to install a virus onto an iVotronic machine: as the EVEREST researchers found, hackers can use a pocket-sized, commercially available personal device to emulate one. A real or forged PEB armed with malicious code could cause any voting machine it interacts with to execute malicious code for any number of purposes—switching votes, erasing votes, breaking down and denying service, taking the system hostage, or otherwise causing havoc during an election. To

compromise a South Carolina election, a bad actor could steal or misappropriate a PEB, or simply gain access to the iVotronic's PEB port for just a moment using a forged device.

52. The security flaws uncovered by the EVEREST researchers are not merely theoretical. After identifying dozens of potentially exploitable vulnerabilities in the iVotronic system's architecture, software, and physical security, the researchers engaged in several exercises designed to simulate actual attacks. The researchers identified and simulated multiple types of hacks that a knowledgeable and motivated hacker could—without the advance provision of code or materials—execute on the currently deployed machines in order to distort or disrupt the election process. The report lists eleven "successful attack scenarios," one of which is denominated "Compromising Entire Election Process with a Virus." *See id.* at 93-99. Because the "ES&S [iVotronic] voting process forms a loop[,] . . . . [i]nserting malicious code at any step in the process could result in a virus spreading to all other components, completely compromising the election." *Id.* at 98.

53. As noted above, South Carolina still conducts elections using iVotronic firmware certified by the SEC in 2006—the very firmware studied and exploited by the EVEREST researchers.

54. Other researchers studying the iVotronic system also found serious security flaws. Following the November 7, 2006 election, the Florida Department of State commissioned a team of researchers at Florida State University ("FSU") to conduct an audit of the 2006 Florida Congressional District 13 election. *See* Florida State University, *Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware*, prepared for Florida Department of State, (Jan. 23, 2007) (hereinafter, "FSU Report").[3] In that

[3] Available online at https://people.eecs.berkeley.edu/~daw/papers/sarasota07.pdf.

congressional race, about 18,000 votes were lost—permanently—from the iVotronic machines. While the FSU researchers had a circumscribed mandate—seeking to determine what caused the votes to disappear—their findings included significant vulnerabilities in the iVotronic's architecture and firmware. Their findings on risks outside of undercounts (*i.e.*, lost votes) are striking because the FSU researchers explicitly did *not* purport to undertake a comprehensive review or audit of the entire iVotronic system.

55. The flaws revealed by the FSU researchers, like those discussed in the EVEREST Report, would provide hackers with lines of attack that could disrupt an election or alter its results. For example, like the EVEREST researchers, they found several different "buffer overflow bugs," software flaws that, once exploited, "can allow an attacker to transfer program control to her own malicious code. Once this happens, the attacker controls the machine." *Id.* at 38. With respect to one particular override bug, the FSU researchers found that "[a]n attacker could use well-known techniques to exploit this bug, inject malicious code into the address space of the iVotronic machine, and cause the processor to begin executing that malicious code. At this point, the attacker has complete control over the iVotronic: the iVotronic is infected." *Id.* at 57. An attacker could inject the virus into a single machine by gaining momentary, unnoticed access, by posing as a technician, or by enlisting help from a voter or poll worker. And in "only seconds," a virus would infect a machine through an attack that "would not necessarily require any kind of suspicious-looking activity." *Id.* A virus could then spread throughout a county's election system, traveling via PEBs to infect other iVotronic machines that then become new hosts for spreading the virus.

56. According to the FSU researchers, an attack along these lines is eminently plausible. Writing in 2007, when nation-state attacks against our election systems likely

seemed far more hypothetical than they do now, the FSU researchers wrote: "Ultimately, our best guess is that discovering this attack would be a matter of technical competence, tedium, and hard work, and it would require considerable motivation, but it would not require genius-level skills. A highly motivated and skilled lone individual could probably do everything needed to exploit the vulnerability. Consequently, the threat cannot be ignored." *Id.* at 58.

Defendants Have Been on Notice of These Vulnerabilities for Years

57. South Carolina's General Assembly and its statewide election officials, including the Defendants in this case, have for years been on notice of the iVotronic system's deep security flaws.

58. In addition to the public reports issued by the Ohio Secretary of State and FSU, the South Carolina General Assembly itself commissioned a review that highlighted the flaws and vulnerabilities of the iVotronic system. In 2013, the General Assembly's Legislative Audit Council ("LAC") published "A Review of Voting Machines in South Carolina" (attached hereto as Exhibit 2.I) ("LAC Report"), a study commissioned by the state Senate's President Pro Tempore. In addition to various "Election Day mishaps" associated with the iVotronic system, the LAC report catalogued studies revealing the iVotronic's deep and systemic vulnerabilities, including the EVEREST and FSU Reports. Based on that review, the LAC's analysis described, among other things, instances in other states of "Vote Flipping," "Candidates missing from screens," "Missing Votes (Undervotes) and Too Many Votes (Overvotes)," and "Election Fraud." LAC Report at 19-20.

59. Two years after the LAC Report, the General Assembly set out again to study the state's election system and concluded that fundamental aspects of it should be replaced. In 2015, it passed legislation establishing a "Joint Voting System Research Committee." *See*

Ronnie Cromer and Walt McLeod, *Report of the Joint Voting System Research Committee*, submitted to the South Carolina General Assembly (Mar. 17, 2016) ("JVSRC Report"), at 2. The legislature required the committee, among other things, to evaluate the state's current voting system, consider best practices identified by the U.S. Election Assistance Commission, and provide "an analysis as to which technology should be implemented in South Carolina." *Id.* at 3.

60. In issuing conclusions and findings, the Joint Committee found "that South Carolina's next voting system must be secure, and instill confidence in the citizens that their votes will be counted, as they intended for them to be cast." *Id.* at 6. It further found that "[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 SEC." *Id.*

61. In preparing its report, the Joint Committee convened two public hearings. At the Committee's second hearing, on November 10, 2015, Defendant Andino submitted testimony that underscored the need to reshape the architecture of South Carolina's voting system. She emphasized that the state's voting system, "[w]ith a life expectancy of approximately 12 to 15 years, . . . is approaching end of life." *Id.* at 9. She also reported that the state's vendor, ES&S, had informed the SEC that "availability of replacement parts will become a problem at some time in the future." *Id.* Indeed, ES&S no longer manufactures the outdated iVotronic machines, and as a result, replacement parts have become older, less reliable, and harder to locate.

62. In her testimony, Defendant Andino outlined a prospective timeline for procurement of new voting machines. She stated that "[t]he optimal date for implementation

of the new system to begin is January 2017," so that it would be in place for its "first statewide use . . . in June of 2018 for the primaries." *Id.* at 10.

63. After that "optimal date" came and went, researchers continued to expose the iVotronic's flaws. In July 2017, the annual DEFCON Hacking Conference, which brings together computer security researchers, featured a "Voting Machine Hacking Village." *See* Matt Blaze et al., "DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure," DEFCON (Sept. 2017) ("DEFCON Report").[4] Participants 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.

64. Under tight time constraints and with no background information, participants identified significant vulnerabilities that could be exploited by hackers. One participant discovered a security flaw in the PEBs, "which is exactly what an attacker seeking to change an election result would attack by changing the firmware in a PEB or swapping a PEB out with a clandestine attacker PEB." *Id.* at 11. One DEFCON attendee tweeted the password for the iVotronic.[5]

---

[4] Available online at https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf.
[5] Lulu Friesdat (@LuluFriesdat), July 30, 2017 12:49 p.m., https://twitter.com/LuluFriesdat/status/891747476343971841.

65. The vulnerabilities identified at the Voting Machine Hacking Village were widely reported in the national news media.[6]

66. On information and belief, Defendants have taken no meaningful steps to address the fundamental security flaws exposed in the EVEREST report, the FSU report, or the DEFCON conference.

South Carolina's Election System is Obsolete and Suffers from Unaddressed Flaws in Maintenance and Security Measures

67. The iVotronic's inherent security deficiencies are exacerbated by the fact that the machines in use in South Carolina have been operating in many instances since 2004, putting them at the end of their lifespan and increasing the prospect of breakdown or failure. As they age, the machines become less reliable and even more susceptible to malicious attack.

68. These machines have failed in ways that impede voting. For example, the LAC Report summarizes "just a few of the repeated errors in South Carolina," which include (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

---

[6] *See*, *e.g.*, Elizabeth Weise, *Hackers at DefCon Conference Exploit Vulnerabilities in Voting Machines*, USA Today (July 30, 2017), https://www.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machines/523639001/; Tom Porter, *Hackers Breach U.S. Voting Machines in 90 Minutes at DefCon Competition*, Newsweek (July 30, 2017), http://www.newsweek.com/hackers-breach-usvoting-machines-90-minutes-def-con-competition-643858; *Hackers Break Into Voting Machines in 2 Hours at Defcon*, CBSNews (July 30, 2017); Kevin Roose, *A Solution to Hackers? More Hackers*, New York Times (Aug. 2, 2017), https://www.nytimes.com/2017/08/02/technology/a-solution-to-hackers-more-hackers.html).

p.m. 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. *See* Caitlin Byrd, *Voting Machine Error Forces Switch to Paper Ballots in Goose Creek Election*, Post and Courier (Apr. 3, 2018).[7]

69. These problems can be expected to grow. Five years ago, the 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." LAC Report at 2.

70. The SEC has begun to observe effects of the aging voting machines on South Carolina's elections. In its "Fiscal Year 2015/16 Accountability Report" it stated that 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." *South Carolina State Election Commission, Fiscal Year 2015-16 Accountability Report* (Sept. 20, 2016), at A-6.[8]

71. In its "Fiscal Year 2016/2017 Accountability Report," the SEC acknowledged that "[t]he useful life of our current 13-year-old voting system is 12 to 15 years." *South Carolina State Election Commission, Fiscal Year 2016-2017 Accountability Report* (Sept. 21, 2017), at A-9.[9] Since "a well maintained voting system is critical to conducting fair and accurate elections," the SEC asserted that "the system requires intensive maintenance and enhancements." *Id.* As a result, the SEC stated its intent to "continue working with the

---

[7] Available online at https://www.postandcourier.com/politics/voting-machine-error-forces-switch-to-paper-ballots-in-goose/article_f5ca1850-3747-11e8-a77a-dfd7f3622aa0.html.
[8] Available online at https://www.scvotes.org/files/Acct%20Report%202015-16%20Final.pdf.
[9] Available online at https://www.scvotes.org/sites/default/files/Combined%20document%20-%202017%20Acc%20Report.pdf.

General Assembly" to secure funding to upgrade and eventually replace the systems. *Id.* It did not, however, set out a concrete timeline for doing so or acknowledge other avenues that it could undertake on its own to discharge its statutory responsibility, such as financing arrangements with vendors for purchasing or leasing new equipment.

72. Local election officials have reinforced this message. In June 2016, Wanda Hemphill, Director of the York County Board of Voter Registration and Elections, wrote to Defendant Andino outlining concerns about the state's aging voting system:

> As a result of the age of our current voting system, we are beginning to see a number of issues for which I have delineated in the attached document. Seeing as we will have this system for some time to come, I think it would be logical to assume that the frequency of most of these issues will increase as the system ages. Due to these issues and the lack of state funding (at this point) for a voting system "refresh," the cost and burden of maintain this system will fall directly on the counties. … [C]ounties are the end users of this dinosaur (affectionately meant) and the entity charged with maintaining and wringing out whatever life remains. But most importantly, we have the financial obligation of this prehistoric relic and the burden of the additional costs it brings.

Email from Wanda Hemphill, Director, York County Board of Voter Registration and Elections, to Marci Andino, Executive Director, South Carolina State Election Commission (Jun. 27, 2016) (obtained via FOIA request). (Attached hereto as Exhibit 2.F.)

73. The document that Ms. Hemphill sent to Defendant Andino spelled out several systemic deficiencies, including some that implicate security. Among other things, the document listing machine issues included "IRV Board Failure (does not recognize PEB)," "Video Board Failures – No display (All White with striations/All Black)," "Exposed wires outside i-Vo casing (after depot)," and PEBs with "No qualifications." *Id.*

74. In 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.[10] Voting machines also broke in Horry, Marlboro, and Florence Counties.[11] Even when the machines did not breakdown entirely, election officials acknowledged that aging touchscreens made it more difficult for voters to make their selections.[12]

Defendants Failed to Take Meaningful Steps to Secure a Vulnerable Voting System

75. For at least a decade, the SEC has been aware of serious deficiencies in the security practices observed by county election officials. These gaps in security are different from, and in addition to, the iVotronic system's inherent security vulnerabilities. In 2008, it conducted a security audit of the state's 46 county election offices. The audit unearthed numerous security risks. Among other things, as summarized in the LAC Report, the audit found "Computers connected to networks or telephone lines that could potentially be used

---

[10] *See* WSPA Staff, "Primary results delayed in Greenville Co. due to broken vote counting machines," WSPA.com (June 13, 2018), *available at* http://www.wspa.com/news/primary-results-delayed-in-greenville-co-due-to-broken-vote-counting-machines/1235223486.

[11] Tyler Fleming, "Gardner declares victory as incumbent awaits a potential new vote count," The Myrtle Beach Sun News (June 13, 2018), *available at* https://www.myrtlebeachonline.com/news/local/article213098414.html; Erin Brown, "Pee Dee counties experience voting machine problems," WBTW News (June 13, 2018), *available at* http://www.wbtw.com/news/pee-dee-counties-experience-voting-machine-problems/1237917971.

[12] Bob Montgomery, "Laye: Voting machines getting older, less sensitive," GoUpstate.com (June 13, 2018), available online at http://www.goupstate.com/news/20180613/laye-voting-machines-getting-older-less-sensitive.

from unsecured or unauthorized access" and poor practices regarding keys and security codes. LAC Report at 14.

76. In the weeks preceding and following the 2016 election, the SEC engaged or coordinated with various state and federal agencies and a third-party cybersecurity vendor to test its cybersecurity program and identify system vulnerabilities. These experts identified numerous security issues, including some declared "critical."

77. One county-by-county review, conducted by the South Carolina National Guard Defensive Cyber Operations Element in October 2016, analyzed every South Carolina county. The review found widely varying levels of physical- and cyber-security vulnerabilities—for example, 20 of the 46 counties had "critical" vulnerabilities related to the Unity software and 21 counties had physical security vulnerabilities (with four described as "critical"). *See* South Carolina National Guard Defensive Cyber Operations Element, *Rapid Vulnerability Assessments of South Carolina's County Election Information Security Posture*, prepared at the request of the South Carolina State Election Commission Executive Director (Oct. 31, 2016) (obtained via FOIA request) (excerpts attached hereto as Exhibit 2.B).

78. The review revealed that many counties maintained systems with vulnerabilities above and beyond the inherent flaws plaguing the iVotronic system, many apparently quite serious. For example, Sumter County had "high" vulnerabilities related to the Unity software and data transfer methods, while Greenville and Charleston Counties, among others, had "critical" Unity-related vulnerabilities. *See* Ex. 2.B. at 4-5, 17, 30. Greenville County also had two "high" physical security vulnerabilities, including one related to "key control of sensitive storage areas." *Id.* at 16.

79. Also in late 2016, the U.S. Department of Homeland Security ("DHS") began producing regular cyber hygiene assessments of the SEC's website and office networks. *See, e.g.*, Department of Homeland Security, National Cybersecurity and Communications Integration Center, "Cyber Hygiene Assessment: SC State Election Commission" (Sept. 18, 2016) ("DHS Report") (obtained via FOIA request); *see also* Alexa Corse, *South Carolina May Prove a Microcosm of U.S. Election Hacking Efforts*, Wall St. Journal (July 16, 2017).[13] The DHS assessments found grave security vulnerabilities plaguing the SEC. For example, the September 18, 2016 cyber hygiene assessment detected 55 vulnerabilities on 3 internet-facing hosts, including two "critical vulnerabilities" and two "high vulnerabilities." DHS Report at 6. The September 25 and October 2, 2016 assessments each also detected two "critical" and two "high" vulnerabilities. *Id.* at 48-49, 89-90. It took the SEC up to 25 days to patch some of these vulnerabilities, a time period that at least one national security official has described as "too long." Corse, *supra*. (Excerpts of the DHS Reports attached hereto as Exhibit 2.A).

80. Indeed, throughout the fall of 2016, Defendants received warnings from multiple sources that the election system faced profound cyber-threats. Sometime around November 1, 2016, the South Carolina Department of Administration relayed a DIS – SEC Assessment and Risk Analysis to Defendant Andino for her review. The report, heavily redacted when released pursuant to FOIA request, categorizes the SEC's infrastructure risk as "high." Three critical vulnerabilities were found (two of which were reportedly remediated in hours). The report also noted that "an appropriate level of security posture commensurate with the high

[13] Available online at https://www.wsj.com/articles/south-carolina-may-prove-a-microcosm-of-u-s-election-hacking-efforts-1500202806.

value systems comprising the [Voter Registration and Election Management System] and SCVotes applications has not been adequately defined." (Attached hereto as Exhibit 2.C).

81. Defendant Andino appeared to object to the tone and presentation of the report. In an email message to Walter Dunbaker of the Division of Information Security, Defendant Andino wrote: "I am deeply concerned and disappointed in the tone as well as the statements and assertions made in the documents. The [SEC] worked together and cooperated fully with the Division of Information Security (DIS) and the Division of Technology (DTO) during this process to identify and remediate vulnerabilities and strengthen our election infrastructure. The draft documents failed to accurately describe the current security posture and does nothing to foster cooperation and build a strong customer/team relationship." She objected to the release of the report and asked for a meeting. (Attached hereto as Exhibit 2.D).

82. These security gaps and vulnerabilities reflect a deficient approach to cybersecurity at the SEC. Media reports and heavily redacted internal documents produced in response to FOIA requests indicate, at best, a belated patching of critical- and high-vulnerability flaws and demonstrate a history of weak cybersecurity initiatives.

The Inherent Insecurity of South Carolina's Voting System is Exacerbated by the State's Inability to Meaningfully Audit Election Results

83. Because 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. In practice, this means establishing robust and consistent audit procedures based on physical evidence of voter intent.

84. Experts in election administration agree that post-election audits are an indispensable element in securing elections against cyberattack.[14] Systematic post-election audits provide election administrators with a method for confirming the initial vote tabulation, an especially vital safeguard for voting systems that electronically record or tabulate votes.

85. To be effective, however, post-election audits must include certain essential elements. First, they must proceed automatically, with clear procedures for the sample size and methods to be used. Second, post-election audits must have clear rules for what happens in the event that an audit is inconsistent with initial results. Third, and most fundamentally, audits must be based on a record of voter intent independent of that saved in each voting machine's software. In practice, this means there must be a paper audit trail.

86. South Carolina does not carry out post-election audits containing any of these necessary elements.

87. Because South Carolina's voting system maintains no software-independent record of voter intent, effective post-election audits simply are not possible using the voting system currently certified by the SEC.

88. In written testimony that Defendant Andino submitted to the Joint Voting System Research Committee, she summarized the SEC's "vision for a new voting system." Among other things, that vision includes a "new voting system [that] will be . . . [a]uditable – the

---

[14] *See*, *e.g.*, Lawrence Norden et al., Brennan Center for Justice, *Post-Election Audits: Restoring Trust in Elections*, (2007), *available at* https://www.brennancenter.org/sites/default/files/legacy/d/download_file_50228.pdf; American Statistical Association, *Statement on Risk-Limiting Post-Election Audits* (Apr. 17, 2010), available at http://www.amstat.org/asa/files/pdfs/POL-Risk-Limiting_Endorsement.pdf; Andy Greenberg, *Hacked or Not, Audit This Election (and All Future Ones)*, Wired (Nov. 23, 2016), https://www.wired.com/2016/11/hacked-not-audit-election-rest/.

system must provide a way to confirm the votes have been cast, recorded and counted accurately (such as a paper record of each vote)." JVSRC Report at 10. And as noted above, that Committee's conclusions and findings stated that "[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 SEC." *Id.* at 6.

89. The current process that the SEC describes as its "election audit" is misnamed. It does not rely on any software-independent source, and thus provides no useful security against cyberattacks or even internal system errors. As described by the SEC, the "audit process" compares tabulated results of the election downloaded from voting machines by PEBs with the data stored on flash cards in the same machines. According to its website, the SEC "has developed a series of computer applications . . . that compares the tabulated returns reports with the raw audit data." *See* SC State Election Commission, *Description of Election Audits in South Carolina* (accessed July 9, 2018).[15] In other words, the SEC compares various components of the iVotronic and Unity systems to determine whether they are internally consistent. *See id.*

90. The "audit process" used by the SEC would not detect any attack on the state's voting system that impacted various system components consistently. As the EVEREST report indicated, the iVotronic system "forms a loop," EVEREST Report at 98, which means that a hack could unfold consistently across the system's components and thereby elude any process designed to detect "anomalies." In other words, in the event of a hack or malfunction, the SEC's audit process would simply check the hacked system against itself.

[15] Available online at https://www.scvotes.org/data/AuditDesc.html.

91. Whatever scant security this audit process might conceivably provide is further diluted by the lack of any clear trigger for further action in the event an anomaly appears. The description of the SEC's "election audits" on its website does not indicate any mechanism for taking action to investigate anomalies within the system. It merely provides that "[i]f the audit application detects an anomaly it lists it in one or more audit report." SC State Election Commission, *Description of Election Audits in South Carolina*. Further, the LAC Report found that, in many instances, local election officials believe they lack adequate time to conduct the SEC's prescribed audit procedures between election day and the statutory deadline to certify election results.

92. More fundamentally, the narrow "audit" procedures imposed by the SEC offer no clear remedy to a cyberattack that infects the state's voting system. Faced with an anomaly—say, a mismatch between the vote count aggregated on a precinct's PEBs and those recorded on the flash drives in that precinct's machines—there is no method for determining which of those sources is authoritative. In this sense, at most, the SEC's audit procedures could demonstrate that an election's results are clouded in doubt—causing precisely the kind of disruption or crisis of confidence that may be a hacker's very purpose—without providing any tools for restoring a proper outcome.

93. South Carolina's failure to provide for meaningful post-election audits compounds the security vulnerabilities endemic to the iVotronic system.

Numerous Sophisticated Adversaries Are Targeting America's Democratic Infrastructure

94. The prospect of cyberattacks on our nation's election systems, whether by nation-states or non-state actors, is immediate and acute. Over the last two years, the persistent

threat to our nation's democratic infrastructure has become severe. As a result, South Carolina's election system is at extraordinary risk. The 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.[16]

95. Federal 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.

96. On February 16, 2018, federal officials indicted 13 Russian nationals and three Russian entities in federal district court in Washington, D.C., in connection with criminal acts aimed at interfering with the U.S. political system. *See* Indictment, *United States v. Internet Research Agency LLC, et al.*, (D.D.C., Feb. 18, 2018) (No. 1:18-cr-00032-DLF).[17] Significantly, though the indictment concerned information operations rather than cyberattacks against election systems, it alleged that in many instances Russian agents acted directly inside the United States or used fraudulent social media accounts to induce Americans inside the United States to act on their behalf.

97. In addition to these so-called "active measures" to influence the American electorate, Russia's well-documented interference has included cyberattacks directed at the nation's election infrastructure.

---

[16] Alexa Corse, *South Carolina May Prove a Microcosm of U.S. Election Hacking Efforts*, W.S.J. (July 16, 2017), *available at* https://www.wsj.com/articles/south-carolina-may-prove-a-microcosm-of-u-s-election-hacking-efforts-1500202806 (quoting Chris Whitmire, the SEC's director of public information and training).

[17] Available online at https://www.justice.gov/file/1035477/download.

98. On August 18, 2016, the FBI issued an advisory entitled "Targeting Activity Against State Board of Election Systems." Alert No. T-LD1004-TT, FBI Flash (Aug. 18, 2016).[18] The advisory reported that "[i]n late June 2016 an unknown actor scanned a state's Board of Election website for vulnerabilities." It went on to request that "states contact their Board of Election and determine if any similar activity . . . has been detected." It also "recommend[ed] that all states" take several specific technical steps to guard against similar cyberattacks.

99. On September 16, 2016, the U.S. Department of Homeland Security ("DHS") issued a press release that reported DHS had detected "efforts at cyber intrusions of voter registration data maintained in state election systems." Press Release, *Statement by Secretary Johnson Concerning the Cybersecurity of the Nation's Election Systems*, Department of Homeland Security (Sept. 16, 2016).[19] The statement also asserted that "we must face the reality that cyber intrusions and attacks in this country are increasingly sophisticated, from a range of increasingly capable actors that include nation-states, cyber hacktivists and criminals."

100. DHS urged state and local election officials to avail themselves of various elements of DHS support in safeguarding their systems against cyberattacks. On January 6, 2017, the Secretary of Homeland Security designated the country's election systems to be "critical infrastructure" pursuant to 42 U.S.C. § 5195c(e). Reflecting the urgency of the threat to election systems, and the vital national interest in protecting those systems, this designation created systems for information-sharing among states and with the federal

---

[18] Available online at https://info.publicintelligence.net/FBI-ElectionHacking.pdf.
[19] Available online at https://www.dhs.gov/news/2016/09/16/statement-secretary-johnson-concerning-cybersecurity-nation%E2%80%99s-election-systems.

government and allowed DHS to prioritize assistance to states seeking help fortifying their election systems.

101. Multiple federal agencies have confirmed that state-sponsored Russian hackers successfully interfered (and made multiple other attempts to interfere) with the 2016 national election. The Central Intelligence Agency ("CIA") issued a report in January 2017 that concluded with "high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election," including "access[ing] elements of multiple state or local electoral boards" and targeting or compromising certain elections-related systems. The CIA concluded that Russia would "apply lessons learned from its campaign aimed at the US presidential election to future influence efforts in the United States and worldwide."[20]

102. In June 2017, *The Intercept* published a previously classified National Security Agency ("NSA") memo describing Russian cyberattacks against American election infrastructure. The report stated that Russian intelligence actors "executed cyber espionage operations against a named U.S. Company in August 2016, evidently to obtain information on elections-related software and hardware solutions, according to information that became available in April 2017." In addition to a spear-phishing campaign against a U.S. company, the Russian agents directed spoofed emails to local election officials. The NSA report stated that "[g]iven the content of the malicious email it was likely that the threat actor was targeting officials involved in the management of voter registration systems. It is unknown whether the aforementioned spear-phishing deployment successfully compromised the

[20] Available online at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

intended victims, and what potential data could have been accessed by the cyber actor." National Security Agency, *Report on Russia/Cybersecurity* (May 5, 2017).[21] *See also* Matthew Cole et al., *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, The Intercept (June 5, 2017).[22]

103. In February 2018, DHS 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." 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).[23]

104. Continuing investigations by Congress into Russia's interference with America's election process have underscored the pronounced and ongoing threat to the country's election infrastructure. On April 27, 2018, the House Permanent Select Committee on Intelligence released its "Report on Russian Active Measures." The committee majority's report, consisting of over 100 pages examining Russia's interference in the 2016 election and its potential for future meddling, discussed the vulnerability of state election systems. Among other things, the committee noted:

> The vulnerability of state and local election infrastructure has been well documented. These systems, which are not frequently updated or replaced, are not developed to defend against state-sponsored cyber threats. The fact that voting machines themselves, as well as tabulation systems, are not directly connected to the internet does not offer adequate security. Rather, it can create a false sense of security.

---

[21] Available online at https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1.
[22] Available online at https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.
[23] Available online at http://subscriber.telegraph.co.uk/news/2018/02/14/russia-could-meddle-us-mid-term-elections-late-secure-now/.

> To help protect the integrity of the process, 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. An example of this is a contemporaneously printed record of votes that is securely stored at the polling place and transported to the relevant election office at the end of Election Day. The Committee is mindful of the reason most jurisdictions replaced the paper ballot, but building in a redundancy using a paper record of a vote will help guard against the potential for manipulation of voting results in the event of a breach of the electronic voting machines.

House Permanent Select Committee on Intelligence, "Report on Russian Active Measures," HRPT-115-1_1-p1-U3 (Mar. 22, 2018), at 123.[24]

105. On May 8, 2018, the Senate Select Committee on Intelligence ("SSCI") released its findings on Russian election interference in a report that set out the stark threat environment currently surrounding election systems. *See* Senate Select Committee on Intelligence, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations" ("SSCI Findings") (May 8, 2018).[25] The SSCI Findings reiterated the conclusion reached over a year ago by the nation's Intelligence Community ("IC"): "In 2016, cyber actors affiliated with the Russian Government conducted an unprecedented, coordinated cyber campaign against state election infrastructure." *Id.* at 1. The report further asserted that "[a]t least 18 states had election systems targeted by Russian-affiliated cyber actors in some fashion. Elements of the IC have varying levels of confidence about three additional states, for a possible total of at least 21. In addition, other states saw suspicious or malicious behavior the IC has been unable to attribute to Russia." *Id.* (internal footnotes omitted).

---

[24] Available online at https://docs.house.gov/meetings/IG/IG00/20180322/108023/HRPT-115-1_1-p1-U3.pdf.

[25] Available online at https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

106. Russia's attacks on state election infrastructure succeeded in penetrating many states' systems. According to the SSCI Findings, "[i]n at least six states, the 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." *Id.* at 1-2 (internal footnotes omitted).

107. As startling as the SSCI Findings were, they did not purport to convey a complete picture of Russia's assaults on American election systems. "The Committee's assessments, as well as the assessments of the [DHS] and the [FBI], are based on self-reporting by the states. DHS has been clear in its representations to the Committee that the Department did not have perfect insight into these cyber activities. It is possible that more states were attacked, but the activity was not detected. In light of the technical challenges associated with cyber forensic analysis, it is also possible that states may have overlooked some indicators of compromise." *Id.* at 2.

108. Just as the SSCI could not be certain whether Russian government-affiliated actors compromised more state systems than detected, it also could not determine the scope of the harm reflected by detected infiltration. The SSCI concluded that "[t]he Committee does not know whether the Russian government-affiliated actors intended to exploit vulnerabilities during the 2016 elections and decided against taking action, or whether they were merely gathering information and testing capabilities for a future attack. Regardless,

the Committee believes the activity indicates an intent to go beyond traditional intelligence collection." *Id*. at 4.

109. The SSCI Findings also noted the connection between a state's voting infrastructure and the risk of cyber-attack. It recognized that "Paperless Direct Recording Electronic (DRE) voting machines—machines with electronic interfaces that electronically store votes (as opposed to paper ballots or optical scanners)—are used in jurisdictions in 30 states and are at highest risk for security flaws." *Id*. at 4. This is exactly the kind of machine used in South Carolina, and South Carolina is one of only five states that uses DREs exclusively. SSCI further noted that "systems that are not connected to the internet, such as voting machines, may still be updated via software downloaded from the internet." *Id.*

110. The SSCI's report called for action by numerous state and federal officials to secure the country's election system in light of the serious threats emanating from Russia and other sophisticated adversaries. Among many other things, it called for immediate-term remedies for precisely the kinds of vulnerabilities plaguing South Carolina's system: "States should rapidly replace outdated and vulnerable voting systems. At a minimum, any machine purchased going forward should have a voter-verified paper trail and no WiFi capability." SSCI Findings at 6.

111. This threat did not abate with the 2016 election. There is broad consensus that Russia, and potentially other foreign state actors, will attempt to interfere in the 2018 election. In an interview with BBC News earlier this year, then-CIA Director Mike Pompeo (who now serves as Secretary of State) warned he had "every expectation" Russia would attempt to interfere with the November 2018 federal elections. *See* Gordon Corera, *Russia*

"Will Target U.S. Mid-term Elections" Says CIA Chief, BBC News (Jan. 29, 2018).[26] Days later, then-Secretary of State Rex Tillerson acknowledged that Russian efforts to disrupt democratic processes across the globe would continue "in the U.S. in 2018." Rich Edson & Nick Kalman, *Russians Already Meddling in U.S. Midterms, Tillerson Says*, Fox News (Feb. 6, 2018).[27]

112. In February 2018, leaders of the U.S. intelligence agencies testified to SSCI that Russia is already "meddling in the midterm elections." Matthew Rosenberg et al., *Russia Sees Midterm Elections as Chance to Sow Fresh Discord, Intelligence Chiefs Warn*, New York Times (Feb. 18, 2018).[28] Director of National Intelligence Dan Coats and other intelligence chiefs laid out two central challenges for the United States: the flow of Russian misinformation and "shoring up the defense of electoral systems, which are run by individual states and were seen as highly vulnerable in 2016." *Id.* Federal Bureau of Investigations Director Christopher A. Wray concurred. *Id*. Numerous other current and former Intelligence Community leaders—including Former Director of the National Security Agency Admiral Michael S. Rogers,[29] National Security Adviser H.R. McMaster, [30] former

---

[26] Available online at https://www.bbc.com/news/world-us-canada-42864372.
[27] Available online at http://www.foxnews.com/politics/2018/02/06/russians-already-meddling-in-us-midterms-tillerson-says.html.
[28] Available online at https://www.nytimes.com/2018/02/13/us/politics/russia-sees-midterm-elections-as-chance-to-sow-fresh-discord-intelligence-chiefs-warn.html.
[29] Aaron Blake, *NSA Director Mike Rogers's Remarkable Comments About Trump's Russia Efforts — or Lack Thereof*, Washington Post (Feb. 27, 2018), https://www.washingtonpost.com/news/the-fix/wp/2018/02/27/nsa-director-mike-rogerss-careful-indictment-of-trumps-anti-russia-efforts/?noredirect=on&utm_term=.44dfef2fd684.
[30] H.R. McMaster, *Russian Aggression is Strengthening Our Resolve,* Atlantic Council, (Apr. 3, 2018), http://www.atlanticcouncil.org/news/transcripts/us-national-security-advisor-lt-gen-h-r-mcmaster-russian-aggression-is-strengthening-our-resolve (warning that "The Kremlin's confidence is growing as its agents conduct their sustained campaigns to undermine our confidence in ourselves and in one another").

CIA Director John Brennan,[31] former Director of National Intelligence James Clapper,[32] former FBI Director James Comey,[33] former DHS Director Jeh Johnson,[34] and others—have publicly concurred.

113. In addition to national security and law enforcement agencies, many members of Congress have recognized the severe threat to our nation's election infrastructure posed by hackers. For example, South Carolina Senator Lindsey Graham, who has co-sponsored federal legislation to help address the threat, has emphasized the gravity of the challenge: "The Russians have been trying to break the backs of democracies all over the world." Press Release, U.S. Senator James Lankford, *Senators Lankford, Klobuchar, Harris, Collins, Heinrich and Graham Introduce Election Security Bill* (Dec. 21, 2017).[35] He has therefore called for legislation that would "defend our elections from foreign interference and sends a strong signal to other bad actors—like Iran and North Korea—that similar acts will not be tolerated." *Id.*

---

[31] Matthew Rosenberg, *Former C.I.A. Chief Tells of Concern Over Possible Russia Ties to Trump Campaign*, New York Times (May 23, 2017), https://www.nytimes.com/2017/05/23/us/politics/congress-testimony-john-brennan-russia-budget.html.

[32] Rachel Martin, *Ex-Intel Chief Clapper Weighs In On Russia Influence Investigation*, NPR Morning Edition, (Feb. 15, 2018), *available at* https://www.npr.org/2018/02/15/585971997/ex-intel-chief-weighs-in-on-russia-influence-investigation.

[33] Full Transcript and Video: James Comey's Testimony on Capitol Hill, New York Times (June 8, 2017), *available at* https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html.

[34] *Open Hearing on Election Security Before the Senate Select Committee on Intelligence*, 115th Cong. (2018) (statement of Former DHS Director Jeh Johnson), *available at* https://www.intelligence.senate.gov/sites/default/files/documents/os-jjohnson-032118.pdf.

[35] Available online at https://www.lankford.senate.gov/news/press-releases/senators-lankford-klobuchar-harris-collins-heinrich-and-graham-introduce-election-security-bill.

114. The vulnerability of voting systems likely makes them particularly attractive targets. As Ambassador James Woolsey, former director of the CIA put it in a 2016 interview: "If I were a bad guy from another country who wanted to disrupt the American system . . . I think I'd concentrate on messing up the touch screen voting systems." Fox Business, *Why a Fmr. CIA Director is Worried About Voting Machines* (Nov. 7, 2016) (starting at 00:54).[36]

CLAIMS FOR RELIEF

Count One

Deprivation of the Right to Vote in Violation of 42 U.S.C. § 1983 and the Due Process and Equal Protection Clauses of the Fourteenth Amendment to the U.S. Constitution

115. Plaintiffs incorporate paragraphs 1-114 by reference.

116. "No right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined." *Wesberry v. Sanders*, 376 U.S. 1, 17 (1964). This fundamental right is protected by the Fourteenth Amendment, including both the Due Process Clause and the Equal Protection Clause.

117. "Obviously included within the right to choose, secured by the Constitution, is the right of qualified voters within a state to cast their ballots and have them counted. . . . " *United States v. Classic*, 313 U.S. 299, 315 (1941). *See also 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."). Further, "the right of suffrage can be denied by a debasement or dilution of

[36] Available online at http://video.foxbusiness.com/v/5199936869001/?#sp=show-clips.

the weight of a citizen's vote just as effectively as by wholly prohibiting the free exercise of the franchise." *Reynolds v. Sims*, 377 U.S. 533, 555 (1964).

118. In South Carolina, the SEC is responsible for approving and adopting a voting system, which includes the system for casting and counting votes, maintaining and producing audit trail information, and identifying voting system components. S.C. Code. §§ 7-13-1655, 7-13-1620.

119. If the SEC determines that a voting system that was previously approved no longer meets the requirements of South Carolina law, it must decertify the system. S.C. Code § 7-13-1620(H).

120. The SEC is "composed of" Defendants Way, Benson, Bowers, and White. S.C. Code § 7-3-10. Defendant Andino, as Executive Director of the SEC, is the commission's chief administrative officer, and South Carolina law provides that she "shall [] supervise the conduct of county board of elections and voter registration . . . and ensure those boards' compliance with the requirements [of] applicable state or federal law." *Id.* § 7-3-20(C)(1).

121. 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.

122. The 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.

123. Defendants have also 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. "Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person's vote over that of another." *Bush v. Gore*, 531 U.S. 98, 104-05 (2000). The Equal Protection Clause forbids the state from administering elections in a manner that results in arbitrary disparities in the accurate recording and tabulating of votes.

124. While the Constitution does not require a state to guarantee perfect accuracy or impregnable safeguards in its election systems, it does require a level of reliability that votes will be accurately counted, and that voters will not face arbitrary and disparate treatment. Defendants have failed to meet these minimal standards. The profound vulnerability of South Carolina's election system reflects the cumulative impact of several interlocking deficiencies:

- The iVotronic system itself contains manifold highly exploitable vulnerabilities. Since at least 2007, experts and researchers have made clear that the iVotronic system is plagued by security flaws that an even moderately skilled attacker could use to compromise both individual machines and the whole iVotronic system, and that a successful cyberattack could undermine an election on a large scale.

- South Carolina's aging machines—many past the manufacturer's anticipated lifespan—have and do malfunction in ways that both impede the voting process and aggravate inherent security vulnerabilities.

- South Carolina lacks the capacity to audit elections. The absence of any record of individual votes, apart from electronic data in the iVotronic's vulnerable and aging software, makes it impossible for the state to detect or remedy the effects of a cyberattack or malfunction.

- Systemic failures to maintain cyber-secure practices by the SEC and among the counties (which the SEC is responsible for overseeing) exacerbate the inherent vulnerabilities of the iVotronic system.

- The current threat environment includes numerous highly sophisticated potential attackers—including nation-states—intent on disrupting state election systems.

125. Plaintiffs are regular South Carolina voters who intend to vote in future elections.

126. As long as South Carolina maintains its current voting system, Plaintiffs will face severe burdens in exercising their right to vote. Simply put, Defendants continued use of a voting system that is dangerously vulnerable to cyber-attack, and that has no meaningful way to detect such an attack, imposes severe burdens on Plaintiffs' fundamental right to vote. The Constitution forbids this.

Prayer for Relief

WHEREFORE, Plaintiffs respectfully request that the Court:

1. Assume jurisdiction over this action;
2. Declare that the 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;
3. Enjoin Defendants from maintaining an election system that fails to reliably record and tabulate votes;
4. Impose injunctive relief requiring Defendants to ensure that Plaintiffs have access to a voting system that will reliably and accurately record and count their votes;
5. Award the Plaintiffs reasonable attorneys' fees and costs pursuant to 42 U.S.C. § 1988; and
6. Any other relief the Court deems appropriate.

(signature page follows)\

Respectfully submitted by,

/s/ Marcus A. Manos_____

Marcus A. Manos (Fed. ID No. 4828)
Victoria L. Eslinger (Federal ID No. #738)
NEXSEN PRUET, LLC
1230 Main Street, Suite 700
Columbia, South Carolina 29201
Telephone: 803.771.8900
Facsimile: 803.253.8277
MManos@nexsenpruet.com
VEslinger@nexsenpruet.com

Laurence M. Schwartztol
(*pro hac vice* forthcoming)
PROTECT DEMOCRACRY PROJECT, INC.
10 Ware Street
Cambridge, Massachusetts 02138
Telephone: 202.945.2092
Facsimile: 929.777.8248
larry.schwarztol@protectdemocracy.org

Anne H. Tindall (*pro hac vice* forthcoming)
Jamila Benkato (*pro hac vice* forthcoming)
PROTECT DEMOCRACY PROJECT, INC.
2020 Pennsylvania Avenue, NW, Suite #163
Washington, D.C. 20006
Telephone: 202.856.9191
Facsimile: 929.777.8428
anne.tindall@protectdemocracy.org
jamila.benkato@protectdemocracy.org

Jessica Marsden (*pro hac vice* forthcoming)
PROTECT DEMOCRACY PROJECT, INC.
106 S. Greensboro St, Suite E
Carrboro, North Carolina 27510
Telephone: 202.672.4812
Facsimile: 929.777.8428
jess.marsden@protectdemocracy.org

David S. Frankel (*pro hac vice* forthcoming)
Samantha V. Ettari (*pro hac vice* forthcoming)
Harry P. Morgenthau (*pro hac vice* forthcoming)
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, New York 10036
Telephone: 212.715.9100
Facsimile: 212.715.8000
dfrankel@kramerlevin.com
settari@kramerlevin.com
hmorgenthau@kramerlevin.com

Hon. Nancy Gertner (Ret.) (*pro hac vice* forthcoming)
FICK & MARX LLP
100 Franklin Street, 7th Floor
Boston, MA 02110
Telephone: 857.321-8360
ngertner@fickmarx.com

Dated: July 10, 2018
Columbia, South Carolina

ATTORNEYS FOR THE PLAINTIFFS