

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF
GEORGIA ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRAD RAFFENSPERGER, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

**CORRECTED JOINT STATEMENT OF ADDITIONAL FACTS IN
SUPPORT OF PLAINTIFFS' OPPOSITIONS TO DEFENDANTS'
MOTIONS FOR SUMMARY JUDGMENT**

Table of Contents

A. DREs Suffered from Serious Vulnerabilities.1

B. Logan Lamb Breaches CES in August 2016.....3

C. Georgia’s GEMS System Was Not Air-Gapped.9

D. Multiple Components of Georgia’s DRE/GEMs Voting System Were Transferred to the Current System.....10

E. Ballots Produced by Georgia’s BMD System are Not Voter-Verifiable, Much Less Voter-Verified.21

F. The July 2021 Halderman Report Identified Numerous Serious Vulnerabilities with Georgia’s Current BMD System.40

G. An Independent Government Cybersecurity Agency Verified Dr. Halderman’s Findings and Recommended Mitigation Measures.51

H. Defendants’ Experts Never Examined Georgia’s Voting Equipment and Admit Key Vulnerabilities.....54

I. Defendants’ Own Cybersecurity Consultant Identified Vulnerabilities.58

J. Georgia’s Election System Lacks Sufficient Safeguards to Protect Against Demonstrated Cybersecurity Vulnerabilities.67

K. The Coffee County Breach Reveals the Lack of Meaningful Safeguards to Protect Georgia’s Voting System.74

 1. Election Officials in Coffee County Permitted Unauthorized Individuals Access to Georgia’s Election System74

 2. Election Data from Coffee County was Uploaded to the Internet and Accessed by Dozens of Unauthorized Individuals.....86

 3. The Coffee County Breach Poses a Serious Threat to the Security of Future Georgia Elections93

L. State Defendants Ignored All Indications of the Coffee County Breach, until Plaintiffs began to Uncover the Facts.....98

M. Georgia’s Election System Also Lacks Procedural Safeguards Because it is Un-Auditable.112

N.	Curling Plaintiffs are Georgia Electors Who Have Suffered Particularized Harm.	117
O.	It is Feasible to Implement a Voting System Using Hand-Marked Paper Ballots in Georgia.	131
P.	State Law Requires Fulton County to Conduct Elections and Implement the Voting System in Fulton County.	135

Plaintiffs respectfully submit this joint Statement of Additional Material Facts as to which there is a genuine issue to be tried in support of their claims in this case and their Oppositions to Defendants' Motions for Summary Judgment.

A. DREs Suffered from Serious Vulnerabilities.

1. The DREs that Georgia used from 2002 until 2019 were vulnerable to numerous routes of infection and attack that are “difficult or impossible to detect or reverse,” Opp. Ex. 1 ¶ 14; see also Opp. Ex. 2 at 7 (this case arose in “a technology context where Georgia’s [then] current voting equipment, software, election and voter databases, are antiquated, seriously flawed, and vulnerable to failure, breach, contamination, and attack.”); Opp. Ex. 3 at PDF p. 108 (2018 National Academies Report finding that voting machines that do not produce a voter-verifiable paper audit trail “be removed from service as soon as possible” and that “[a]ll local, state, and federal elections should be conducted using human readable paper ballots by the 2020 presidential election.”).

2. The bootloader software used in Georgia’s DREs dates from June 2002 and was not updated for the 18 years that Georgia used DREs as the primary voting method. The bootloader software is critical to the DREs’ security since it

runs every time they are powered on and controls sensitive operations such as loading the operating system and installing software updates. Opp. Ex. 4 ¶¶ 26-29.

3. The BallotStation election software installed on Georgia’s DREs was not materially updated since 2004. Opp. Ex. 4 ¶¶ 27-29.

4. The Diebold AccuVote TSX vulnerability discovered by Harri Hursti in 2006 and described by Michael Shamos as “one of the most severe security flaws ever discovered in a voting system” is present in the DREs software that was used in Georgia until 2020. Diebold released a patch to address the vulnerability in 2006 but Georgia never installed it. Opp. Ex. 5 at 115-17; Opp. Ex. 6 at 2; Opp. Ex. 2 at 23-24; Opp. Ex. 4 ¶¶ 27-29; *see also* Opp. Ex. 7 ¶¶ 8-9; Opp. Ex. 1 ¶ 18.

5. Diebold’s AccuVote TSX DRE machine was vulnerable to malware that could infect machines and steal votes in a manner that ensured the attacker’s favored candidate always had at least a certain percentage of the vote total. The malware could modify all of the vote records, audit logs, and protective counters stored by the machine, so that even careful forensic examination of the files would find nothing amiss. The voting machine virus could spread the vote-stealing malware automatically and silently from DRE machine to DRE machine during

normal election activities via the removable memory cards. Opp. Ex. 6 at 2; Opp. Ex. 4 ¶¶ 27-29; Opp. Ex. 8 at 1-2; *see also* Opp. Ex. 1 ¶¶ 18-21.

B. Logan Lamb Breaches CES in August 2016.

6. From approximately 2002 to 2017, the Secretary of State contracted with Kennesaw State University's ("KSU") Center for Elections System ("CES") to manage the GEMS/DRE system for all 159 Georgia counties. Opp. Ex. 9 at 107-09; Opp. Ex. 10 at 8:17-9:7; Opp. Ex. 11 ¶ 2; *see also* Opp. Ex. 12.

7. On August 24, 2016, Logan Lamb, a professional cybersecurity expert, was able to access, through the CES public website, "key election system files, including multiple gigabytes of data and thousands of files with private elector information [including] electors' driver's license numbers, birth dates, full home addresses, the last four digits of their Social Security numbers, and more." Opp. Ex. 2 at 64; Opp. Ex. 13 at 8; Opp. Ex. 14 ¶¶ 12-15; Opp. Ex. 4 ¶ 24.

8. Mr. Lamb "was also able to access, for at least 15 counties, the election management databases from the GEMS central tabulator used to create ballot definitions, program memory cards, and tally and store and report all votes." Opp. Ex. 2 at 64; Opp. Ex. 13 at 8; Opp. Ex. 14 ¶ 14(b).

9. Additionally, Mr. Lamb was “able to access passwords for polling place supervisors to operate the DREs and make administrative corrections to the DREs.” Opp. Ex. 2 at 64; Opp. Ex. 13 at 8; Opp. Ex. 14 ¶ 14(d).

10. On August 28, 2016, Mr. Lamb alerted Merle King, the Executive Director who oversaw CES, of the system’s vulnerabilities. Opp. Ex. 15 ¶ 5; Opp. Ex. 2 at 64; Opp. Ex. 13 at 8; Opp. Ex. 14 ¶ 16; Opp. Ex. 16 at 432-33; Opp. Ex. 17.

11. KSU’s CES did not take successful remedial action after Mr. Lamb alerted Mr. King of the vulnerabilities. Opp. Ex. 14 ¶ 16; *see also* Opp. Ex. 2 at 64; Opp. Ex. 13 at 8.

12. A colleague of Mr. Lamb’s, Chris Grayson, was able to repeat Mr. Lamb’s actions in February 2017. Opp. Ex. 2 at 64; Opp. Ex. 13 at 8; Opp. Ex. 14 ¶ 16.

13. Mr. Lamb was also able to access and download the above information in the same manner around February 2017. Opp. Ex. 2 at 64; Opp. Ex. 13 at 8; Opp. Ex. 14 ¶ 16.

14. On March 1, 2017, Mr. Grayson notified KSU of the open access to the “elections.kennesaw.edu” server. Opp. Ex. 16 at 422-25, 433-35.

15. On March 2, 2017, the KSU University Technology Services (“UTIS”) Information Security Office “pulled apache and Drupal logs...and seized the ‘elections.kennesaw.edu’ server.” Opp. Ex. 16 at 422-25.

16. On March 3, the FBI was contacted, and FBI took possession of “the impacted server;” the evidence suggests that only a single server was turned over to the FBI. Opp. Ex. 16 at 422-25; *see also* Opp. Ex. 2 at 64; Opp. Ex. 13 at 8-9.

17. A Forensic image of this server was created on March 6, 2017, by the FBI. Opp. Ex. 18 ¶¶ 7, 10.

18. The FBI returned the seized server to KSU on March 17, 2017, at the prompting of Michael Barnes, who expressed a need to access data on the compromised server. Opp. Ex. 18 ¶ 28; Opp. Ex. 19.

19. Data from the compromised KSU server was retrieved at the direction of Michael Barnes including a directory that contained “workflow databases used during our ballot building efforts.” Opp. Ex. 18 ¶ 28; Opp. Ex. 19.

20. On July 7, 2017, the day after a copy of the Complaint in this action was served to the Secretary of State’s Office, all the data on the hard drives of Kennesaw State University’s server were destroyed. Opp. Ex. 20; Opp. Ex. 21; Opp. Ex. 2 at 65; Opp. Ex. 13 at 9.

21. On August 9, 2017, less than one day after this action was removed to this Court, all the data on the hard drives of a secondary server, containing similar information, were also destroyed. Opp. Ex. 2 at 65; Opp. Ex. 13 at 9; Opp. Ex. 22; Opp. Ex. 23.

22. State Defendants contended that the KSU servers were simply “repurposed” (after the SOS’s Office first attributed the wiping of the servers to “undeniable ineptitude”), but after carefully reviewing the evidence, this Court determined that contention was “flatly not credible.” Opp. Ex. 10 at 111:10-14; Opp. Ex. 24 at 2; Opp. Ex. 2 at 70-71; Opp. Ex. 25.

23. Despite the data on the original server and the backup server having been purposefully destroyed, Logan Lamb, on January 1, 2020, was able to begin a forensic audit of the March 6, 2017 forensic image created by the FBI. Opp. Ex. 18 ¶¶ 7-9.

24. There is evidence that on December 2, 2014, an attacker was able to breach the KSU server and exploit the “shellshock” bug, well before the 2016 election. Opp. Ex. 18 ¶¶ 11(a), 13, 15-20; Opp. Ex. 4 ¶ 23.

25. Despite significant media attention and warnings from the Department of Homeland Security, CES did not take action to patch the “shellshock” bug before December 2014. Opp. Ex. 18 ¶¶ 13-14.

26. If an attacker did indeed exploit the “shellshock” bug, then they would have had almost total control of the KSU server including the abilities to modify files, delete data, and install malware. Opp. Ex. 18 ¶ 20.

27. The access log records on the forensic image of the KSU server only go back to November 10, 2016, two days after the 2016 election. The missing logs could be vital to determining if the server was breached on additional occasions

before the election, and there were no legitimate reasons why records from that critical period of time should have been deleted. Opp. Ex. 18 ¶¶ 11(b), 21-22; Opp. Ex. 4 ¶ 22; Opp. Ex. 1 at 61-62, 66-68.

28. The forensic image from the FBI reveals that there were “scores of files” deleted on March 2, 2017, just before the server was taken offline by the CES/KSU staff and the original server handed over to the FBI. Opp. Ex. 18 ¶¶ 11(c), 24.

29. The installer file for the BallotStation election software used on the DREs was publicly available on the KSU server, where it could have been modified by a malicious actor. Opp. Ex. 18 ¶¶ 11(d), 25-27; Opp. Ex. 4 ¶ 28.

30. The KSU server was used to regularly exchange e-pollbook information with counties. Opp. Ex. 26 at 183:10-25, 184:7-11; Opp. Ex. 10 at 110:9-16; Opp. Ex. 27 ¶¶ 4-5; Opp. Ex. 28 at 1-2 (Instructions from KSU on how to transfer files via USB drive from GEMS server to external computer for upload).

31. In 2018, Mr. Lamb concluded that: “The [DRE/GEMS] system is flawed by design and made worse by the KSU exposure in ways that cannot be practically mitigated. The system should be treated as untrustworthy for the conduct of Georgia’s elections.” Opp. Ex. 14 ¶ 23.

C. Georgia’s GEMS System Was Not Air-Gapped.

32. USB drives used with the GEMS servers were formatted using SOS public-facing computers that are connected to the internet before being used directly with the GEMS system. Opp. Ex. 29 at 77-78; 101:3-9, 107:1-4; *see also* Opp. Ex. 2 at 26-33.

33. Outside contractors built ballots on Georgia’s GEMS database using their personal computers in their homes, and those ballot files were then uploaded to state and county voting equipment. Opp. Ex. 29 at 83:24-85:21.

34. If malware ends up on the memory cards, it can be propagated between GEMs and the DREs. Opp. Ex. 5 at 119:12-15.

35. James Oliver, the SOS's former Security Manager, did not know if Georgia's election management server was air gapped and was not involved in any efforts to air gap the server. Opp. Ex. 30 at 96:13-98:8.

36. Merritt Beaver, the SOS's long-running CIO, could not say for sure that no one in any of the counties connected any part of the system to the internet or internet-equipped devices. Opp. Ex. 31 at 11:9-12:15, 46:20-48:25, 133:7-11; Opp. Ex. 32; Opp. Ex. 33.

37. Georgia election results were sent over phone lines from a modem connected to the GEMS servers. Opp. Ex. 26 at 265:20-267:3.

D. Multiple Components of Georgia's DRE/GEMs Voting System Were Transferred to the Current System.

38. Georgia's voter registration database, ElectionNET ("ENET"), was used by county registrars with the DRE system and BMD system to maintain and update voter registration records and determine ballot precinct information. Opp. Ex. 4 ¶ 66; Opp. Ex. 34 at 23; *see, e.g.*, SMF Exs. 18, 21, 23, 24, 29, 32, 34, 36 (ENET reports of individual plaintiffs); *see also* Opp. Ex. 2 at 69 ("The programming and use of ballots in both the DRE and the Dominion BMD system

is inherently tied to the accuracy of voter precinct and address information in the voter registration database, and inaccuracy in this voter information triggers a variety of obstacles in the voting process”), 88 (noting that ENET “plays a vital role in the proper functioning of the voting system”).

39. ElectioNET contains the personal identifying information of millions of Georgia voters and “plays a vital role in the proper functioning of the voting system.” Opp. Ex. 35 ¶ 3; Opp. Ex. 2 at 88; *see, e.g.*, SMF Exs. 18, 21, 23, 24, 29, 32, 34, 36 (ENET reports of individual plaintiffs).

40. The programming and use of ballots in both the DRE and the Dominion BMD system is inherently tied to the accuracy of voter precinct and address information in the voter registration database, and inaccuracy in this voter information triggers a variety of obstacles in the voting process. Opp. Ex. 36 at 155:16-15 (Rick Barron testifying to the issues Fulton County experienced with the electronic pollpads in the September 2020 election); *see also* Opp. Ex. 2 at 88-89.

41. ElectioNET “had rampant security issues” that made it possible for unauthorized parties to access and modify sensitive system configuration files and voter registration data and create absentee ballot requests for other voters. Opp.

Ex. 4 ¶¶ 66-68; Opp. Ex. 29 at 38:5-40:5, 226:1-227:8; Opp. Ex. 37; Opp. Ex. 38 at 21; Opp. Ex. 39; Opp. Ex. 31 at 169:8-23; Opp. Ex. 40; Opp. Ex. 41; Opp. Ex. 42; Opp. Ex. 49; *see also* Opp. Ex. 43 at 16-17; Opp. Ex. 2 at 7 (finding “the record demonstrates the perilous vulnerability and unreliability of the State’s electronic voter registration system as well as its burdening of Georgia citizens’ right to cast a vote that reliably will be counted”), 88 (finding Georgia’s ENET system “has been open to access, alteration, and likely some degree of virus and malware infection for years,” including vulnerabilities which were not addressed even after the CES/KSU functions were transferred back to the SOS), 149 (“voter database problems extensively identified” in this case “present an imminent threat to voters’ exercise of their right to vote”).

42. Voter registration information was retrieved from ENET via USB drives to update the ExpressPoll pollbooks used in the DRE system. Opp. Ex. 26 at 185:2-5, 211:1-12; Opp. Ex. 29 at 104:23-105:3, 106:1-6; Opp. Ex. 44 at 332:4-6.

43. The voter registration system, ENET, shared or exchanged files with the KSU server that was “wide open to the world for at least six months from

August 2016 to March of 2017,” including sensitive personal information for millions of voters. Opp. Ex. 26 at 184:7-185:4; Opp. Ex. 14 ¶ 14(a).

44. After the SOS took over operations from KSU in 2017, files were retrieved from the same voter registration system, ENET, and sent via FTP from the SOS server to counties with instructions to save the files to their local desktops in order to update the ExpressPoll pollbooks used in the DRE system. Opp. Ex. 28 at 7, 3-16.

45. For at least three years, ENET has been used to update the new KNOWInk PollPad pollbooks used with the BMDs. Opp. Ex. 45 ¶ 8; Opp. Ex. 43 at 16-17; Opp. Ex. 46 at 3; Opp. Ex. 27 ¶¶ 2-3.

46. ENET was not replaced with the adoption of the Dominion BMD election system; until late January 2023, county registrars continued to use the same voter registration database to maintain voter registration records, determine ballot precinct information, and load that information onto poll pads. Opp. Ex. 31 at 183:2-184:18; Opp. Ex. 47 at 11 n.14 (“KNOWink Poll Pads, which will receive text-file data from ENET after the security scans required by Georgia law is completely replacing the ExpressPoll system.”); Opp. Ex. 35 ¶ 12; *see also* Opp.

Ex. 34 at 23 (“Other than a switch to the new KnowInk PollPad electronic pollbooks, Defendants have offered nothing to indicate concretely any action taken in response to issues experienced by voters in November 2018 and more recent elections to ensure that the information from ENET and the operation of the electronic pollbooks is reliable, accurate, and updated.”).

47. There is no evidence the State took any actions to address the deficiencies in the voter registration database. *See* Opp. Ex. 48 at 10:19-12:23; 192:17-194:9; Opp. Ex. 32; Opp. Ex. 33; Opp. Ex. 31 at 6-8, 16, 18, 19, 21; Opp. Ex. 49; *see also* Opp. Ex. 4 ¶ 12; Opp. Ex. 50 at Response No. 65; Opp. Ex. 51 at 23 (this Court previously “required State Defendants to develop procedures and take other actions to address the significant deficiencies in the voter registration database,” but “it [wa]s unclear what actions, if any, the State has undertaken to address these deficiencies . . . in advance of” the 2020 elections.”).

48. Fortalice recommended an additional authentication mechanism for the voter registration database in at least October 2017. Opp. Ex. 38 at 24. Two factor authentication for ENET was not implemented until July 30, 2018. Opp. Ex. 52 at 5; Opp. Ex. 28 at 15-16.

49. In at least December 2020, Secretary Raffensperger certified that the “Voter Registration System is being maintained in a manner consistent with the standards set forth in subsection (b) of this rule [SOS Rule 590-8.3]” despite warnings from the SOS Chief Information Security Officer that the voter registration system was unable to meet SOS rule requirements. Opp. Ex. 31 at 170:18-187:16; Opp. Exs. 42, 49, 53.

50. While the SOS’s office recently indicated that it is phasing out ENET, the extent of data from ENET already transferred over to the BMD system remains unclear. Opp. Ex. 31 at 182:18-184:18; Opp. Ex. 54 ¶¶ 10-11; Opp. Ex. 4 ¶ 12.

51. State Defendants have offered no information to show that no corrupt or infected data from ENET will be transferred over to the new voter registration system. Opp. Ex. 4 ¶ 12; *see also* Opp. Ex. 2 at 89 (stating that simply purchasing now poll machines from Dominion as part of a new contract “cannot alone cleanse the voter database to be transferred and relied upon.”).

52. One of several ways in which the Dominion BMD system could potentially be attacked is using an attack facilitated by a preexisting infection of

the DRE/GEMS system. Opp. Ex. 55 at 36:9-13, 37:6-8; Opp. Ex. 27 ¶¶ 2-3; Opp. Ex. 56 at 119:18, 121:23-122:3; Opp. Ex. 14 ¶ 14.

53. Despite the purchase and deployment of new equipment for Georgia's current election system, important databases, files, and personnel were carried forward from the previous election system (the "GEMS/DRE System"). Opp. Ex. 57 ¶ 3; Opp. Ex. 31 at 20:11-15, 21:7-9, 27:16-30:2, 44:6-13; Opp. Ex. 58; Opp. Ex. 4 ¶ 12; Opp. Ex. 27 ¶ 4.

54. The DRE/GEMS system was unpatched for most of a 15-year period, during which it potentially could have been compromised by many kinds of sophisticated attackers who would then still have a way into the system that would facilitate remaining inside or remaining in a position of having infiltrated the Georgia election system into the current day. Opp. Ex. 55 at 36:14-37:8.

55. This means that vulnerabilities in the GEMS/DRE System will also affect the security of the current election system. Opp. Ex. 57 ¶ 3; Opp. Ex. 27 ¶ 4 ("Although the KSU server itself was decommissioned in 2017, many of these potentially infected computers likely remain in use with the BMD-based system."); Opp. Ex. 18 ¶¶ 29-30 ("It is unreasonable to assume that the new BMD election

system and supporting infrastructure is not already potentially compromised or exposed to malware or given the broad range of election files on the CES elections.kennesaw.edu server.”); Opp. Ex. 54 ¶ 10; Opp. Ex. 59 ¶¶ 5-10.

56. The SOS’s legacy GEMS server was not shut down when it was replaced, and was located within the same room at the Elections Center as the current EMS Server that runs Dominion’s Democracy Suite. Opp. Ex. 165; Opp. Ex. 61; Opp. Ex. 62; Opp. Ex. 31 at 246:16-247:8.

57. It was common for election workers to re-use old USB drives (used with GEMS) in uploading the Election Night Reporting system from the Dominion EMS, permitting malware to travel from the old GEMS system to the ENR webserver to the Dominion EMS and BMD system. *See, e.g.*, Opp. Ex. 31 at 28:11-20, 34:3-35:15; Opp. Ex. 62; Opp. Ex. 63 at 36:4-38:3; Opp. Ex. 64; Opp. Ex. 65; Opp. Ex. 66; Opp. Ex. 28 at 1-2 (GEMS USB drives potentially used with compromised KSU server).

58. After finding a box containing flash drives predating his employment in the server room, James Barnes plugged one into the EMS to copy election project files during an election. Barnes is unsure of the origin of these flash drives

and whether they were appropriate to use with Georgia' voting system. Opp. Ex. 67 at 193:25-195:13.

59. The build instructions for the new EMS server list the "[REDACTED]" because they "[REDACTED]" Opp. Ex. 62.

60. Removeable media could spread vote-stealing malware to BMDs throughout a county or the state if connected to a central EMS server at the state or county level. Dkt. 1131 at 12¹.

61. Consumer grade USB flash drives are used to transfer data from the Elections Center's EMS "[REDACTED]." State Defendants' former Chief Information Security Officer acknowledged: "[REDACTED]" Opp. Ex. 68.

¹ Dr. Halderman's July 1, 2021, report contains the substance of testimony he will offer at trial. *See Pritchard v. Southern Co. Services*, 92 F.3d 1130, 1135 (11th Cir. 1996) (noting that written testimony "can be reduced to admissible form at trial" by calling the testifier as a witness).

62. Data has moved into and out of what was supposed to be—but was not—an “air-gapped system” using removable media that were provided by the SOS’s office (and potentially other sources). Opp. Ex. 69 at 122:15-125:6; Opp. Ex. 70 at 34:5-14.

63. Georgia’s use of “commodity USBs” to move data into and out of the purportedly “air-gapped” election system was not a competent or safe security practice because, *inter alia*, the USBs were not made in the U.S. and could have had data or malware already stored on them. Opp. Ex. 69 at 122:15-125:6.

64. The SOS’s Chief Information Security Officer, David Hamilton, recommended that the SOS adopt a more secure “managed USB” program through a vendor called Datalocker, but that had not been implemented by the time he left in 2021. Opp. Ex. 69 at 122:15-125:6.

65. Infiltration of Georgia’s current BMD-related election hardware could be easily accomplished in under two minutes simply by plugging in a USB drive containing malicious code into a USB port on the equipment, including by a voter in the voting booth. *See* Dkt. 1131 at 46-48; Opp. Ex. 146 § 2.2.1, § 2.2.3, § 2.2.4, § 2.2.5, § 2.2.7.

66. Such malware has the potential to be installed by dishonest election workers (or what Defendants refer to as “insiders”) or intruders who gain access to the machines during pre-election testing and at the polling place. Opp. Ex. 5 at 82:1-20; Opp. Ex. 71 at 102:8-23; *see also* Dkt. 1131 at 48.

67. The software on BMD machines is updated with a USB device that is plugged into each machine. Opp. Ex. 70 at 33:22-24.

68. Fulton County does not scan or inspect the USB devices used to update the software on BMD machines. Opp. Ex. 70 at 34:5-14.

69. Using fresh USB devices in every election would be a prudent security recommendation, but Defendants do not do this. Opp. Ex. 56 at 126:5-20.

70. It would be a cause for concern if poll workers in Georgia were connecting USB drives to voting equipment that had also been connected to internet-connected devices (which they have). Opp. Ex. 56 at 126:21-127:16.

71. It would be a cause for concern if election workers in Georgia publicly shared or otherwise disclosed to unauthorized personnel passwords used

to access and operate voting equipment (which they have). Opp. Ex. 56 at 127:17-128:7.

72. Coffee County employee Misty Hampton publicly shared a YouTube video in which two passwords used to access and operate voting equipment (including the critically-important county EMS server) were readily visible to viewers. Opp. Exs. 72, 73, 74; Opp. Ex. 75 ¶¶ 53-57; Opp. Ex. 76 at 5-8.

E. Ballots Produced by Georgia’s BMD System are Not Voter-Verifiable, Much Less Voter-Verified.

73. Georgia used a DRE in-person voting system for all elections conducted in the state from 2002 until 2019, when this Court granted Plaintiffs’ request for an injunction against the continued use of that system. Opp. Ex. 9 at 101; Opp. Ex. 2 at 147-48. Secretary Raffensperger admitted that Georgia ended its use of the DRE system at the direction of this Court. Opp. Ex. 77 at 6; Opp. Ex. 78 at 11 (“We stood up a new voting system, new voting machines in less than six months. *And that was really because we had an activist federal judge that said you can’t use the old DRE machines. And so we had to do that for the first primary that we had coming up.*”) (emphasis added); *see also* Opp. Ex. 79 at 8 (State was “aware of the [2018] order in *Curling v. Kemp* [that] strongly suggest[ed] that if

Georgia does not update its voting system soon, a new system will be ordered”); Opp. Ex. 80 at 4-5 (State Defendants admit “the Order prevents the GEMS/DRE system from being used in 2020 elections”).

74. This Court’s 2019 injunction against that system still stands today. Opp. Ex. 2 at 147-48, 152.

75. In April 2019—in the wake of this Court’s September 2018 preliminary injunction Order (Opp. Ex. 302 at 109-12) which found serious security and reliability failings with Georgia’s DRE/GEMS system and warned Defendants that prompt corrective action was needed and expected—H.B. 316 was adopted, which provided for the DRE/GEMS system to be replaced with Dominion’s Democracy Suite BMD system, including optical scanners, for all in-person voters in state and federal elections. O.C.G.A. § 21-2-300(a)(2); Opp. Ex. 81 at 3.

76. The following business day after the July 25-26, 2019 hearing that culminated in this Court granting an injunction barring the continued use of DREs, Secretary Raffensperger announced his selection of Dominion’s Democracy Suite system for Georgia elections. Opp. Ex. 82.

77. On July 29, 2019, the Secretary of State's Office posted the Notice of Intent to Award (NOIA) the contract for the State's new voting system including all equipment and software components to Dominion Voting Systems, Inc. ("Dominion"). Opp. Ex. 199; *see also* Opp. Ex. 84.

78. The final Notice of Award and certification was awarded to Dominion on August 9, 2019. Opp. Ex. 83.

79. Georgia's Dominion BMD system encompasses but is not limited to: ImageCast X Prime (ICX) BMDs and associated printers, ImageCast Central (ICC) central-count optical scanners, Image Cast Precinct (ICP) precinct-count optical scanners, and the Democracy Suite election management system (EMS) software. Opp. Ex. 84 at 52-58; Dkt. 1131, Halderman Report at 9.

80. Dominion's Democracy Suite EMS software is used to create election definition files containing information specific to each election, which are loaded onto each BMD from a USB drive before each election. Dkt. 1131, Halderman Report at 10; Opp. Ex. 84 at 54 (ImageCast X-Prime BMD "The ballot is loaded directly onto the standalone device"), 100 ("Load Elections Files on USB").

81. Both BMD-printed ballots and handmarked paper ballots (“HMPBs”) are fed into an ICC or ICP scanner, which is supposed to tabulate them and deposit them into a ballot box. Opp. Ex. 84 at 54-55; Dkt. 1131, Halderman Report at 11.

82. The ICX BMD requires voters to make selections on a large computer screen that can be visible to other voters while the voter makes their selections; the BMD is supposed to cause an attached non-proprietary printer connected to the BMD by a cable to print ballots. Opp. Ex. 84 at 54 (listing 21.5” Avalue touchscreen, HP LaserJet Pro M402dne laser printer and 6’ cable); Dkt. 1131, Halderman Report at 10-11, 18.

83. The system described in Georgia’s contract with Dominion calls for in-precinct scanners/tabulators to count votes based on 2D QR barcodes included on the printed ballots generated by the BMDs. Opp. Ex. 84 at 54; Dkt. 1131, Halderman Report at 13-14; SMF Ex. 4 ¶ 9.

84. The BMDs, Image Cast X models, also produce what is supposed to be a text summary of an elector’s candidate selections on the printed ballots. Opp. Ex. 54 ¶ 37; SMF Ex. 4 ¶ 4.

85. Each printed ballot is supposed to contain both a 2D QR barcode and human-readable text, both of which are supposed to capture the voter's selections made on the BMD touchscreen. Dkt. 1131, Halderman Report at 13-14; Opp. Ex. 54 ¶ 37; Opp. Ex. 84 at 54; SMF Ex. 4 ¶ 4.

86. The Dominion ICP and ICC scanners currently used in Georgia can already scan and tabulate votes using paper ballots without QR barcodes. SMF Ex. 4 ¶ 4; Opp. Ex. 36 at 79:15-18; *see also* Opp. Ex. 54 ¶¶ 4, 37-40; Opp. Ex. 57 ¶ 11.

87. Currently in Georgia, the ballot scanners tabulate votes from each BMD-produced ballot based on the 2D QR barcode generated by the BMD, and not based on the human-readable text. Dkt. 1131, Halderman Report at 13-14, ¶ 7; Opp. Ex. 84 at 54; Opp. Ex. 54 ¶ 32; SMF Ex. 4 ¶ 9.

88. Electors cannot visually review and confirm whether the barcode accurately conveys their selections. Dkt. 1131, Halderman Report at 13-14; Opp. Ex. 57 ¶¶ 3-8, 12-15, 20, 22; Opp. Ex. 56 at 38:2-7, 55:23-57:2; Opp. Ex. 85 at 10:1-17, 25:22-26:20, 71:3-72:8; Opp. Ex. 32; Opp. Ex. 33; Opp. Ex. 70 at 180:20-181:7; Opp. Ex. 86; SMF Ex. 55 at PDF p. 4, ¶¶ 9-10; Opp. Ex. 87 at 46:4-11; Opp. Ex. 5 at 56:13-57:21; Dkt. 1131 ¶ 3.2; Opp. Ex. 57 ¶ 6; Opp. Ex. 88 ¶ 27;

Opp. Ex. 89 ¶ 18; SMF Ex. 42 ¶ 87(b); Opp. Ex. 90 ¶ 10; SMF Ex. 59 ¶ 54; Dkt. 1590-7, Feb. 2023 Marks Decl., Ex. 7 at 4 *see also* Opp. Ex. 2 at 9 n.10 (finding “no elector can visually review and confirm whether the barcode accurately conveys her votes actually cast, as filled out on the BMD screen or appearing on the printout.”); Opp. Ex. 91 at 82 (“the evidence shows that the Dominion BMD system does not produce a voter-verifiable paper ballot or a paper ballot marked with the voter’s choices in a format readable by the voter because the votes are tabulated solely from the unreadable QR code”); *id* at 147 (“Time will tell whether Act V here can be still avoided or at least re-written.”).

89. Dr. Alex Halderman identified an instance where a QR code on a ballot cast in DeKalb County did not match the human readable text on that ballot. Dkt. 1590-13 (June 7, 2022 Jan. 20, 2023 email from Halderman to Marks); Dkt. 1590-12, Feb. 2023 Marks Decl., Ex. 12 at 2; *see also* SMF Ex. 42 ¶ 87(b)(i); Dkt. 1131 ¶¶ 5, 7

90. Most voters do not verify that the human readable portion of their printed ballots reflect their intended votes. Opp. Ex. 70 at 180:20-181:13; Opp. Ex. 54 at ¶ 7(b), 21 n.40 (citing Opp. Ex. 27 at Ex. A); SMF Ex. 55 at PDF p. 53, ¶ 22; Opp. Ex. 92 at 1-2; Opp. Ex. 56 at 70:20-72:2; Opp. Ex. 93 ¶¶ 10, 63-64;

Opp. Ex. 71 at 75:2-7; Opp. Ex. 87 at 46:12-21; Dkt. 1589-4, Feb. 2, 2023 Stark Decl., Ex. 4 (Georgia Verification Study) at 3; Opp. Ex. 54 ¶ 7(b); Dkt. 1593, Feb. 2023 Dufort Decl. ¶ 34; Dkt. 1597, Feb. 2023 Nakamura Decl. ¶ 48.

91. Multiple studies of the BMD system in practice show that the rates at which voters typically check the human-readable text on the ballots (when they check at all) fall far short of the rates election security experts agree is needed to detect a systematic problem with Georgia's voting system and to allow for any remedy to correct the problem. *See* SMF Ex. 59 ¶¶ 60-64; *see also* Opp. Ex. 94.

92. Even if a voter checks their ballot, they are unlikely to spot errors and are very unlikely to raise the issue to a poll manager, and even if they do, they are likely to simply be directed by election workers to spoil their ballot and vote again rather than corrective action being taken to address a failure with the voting equipment or broader system itself. SMF Ex. 59 ¶¶ 22, 65-74; Opp. Ex. 87 at 44:21-45:16, 47:11-15; Opp. Ex. 92 at 2; *see also* Opp. Ex. 4 ¶ 7.

93. In the Georgia Voter Verification Study commissioned by the SOS's Office, *only 19%* of voters checked their ballots for *more than five seconds*. Dkt. 1589-4, Feb. 2, 2023 Stark Decl., Ex. 4 (Georgia Verification Study) at 2-3. When

State Defendants' expert Juan Gilbert was asked in his deposition to look at a real, BMD-printed ballot cast in Fayette County during the November 2020 election and *just identify the candidates selected who were not Republicans*, it took him *21 seconds* to be able to do so with just the one ballot. Opp. Ex. 71 at 180:7-24; Dkt. 1131 at 15.

94. BMD-printed ballots can be particularly difficult to read and understand. Opp. Ex. 93 ¶ 8; Opp. Ex. 3 at PDF p. 107 n.75; Opp. Ex. 56 at 36:15-37:2, 71:17-72:2; Opp. Ex. 87 at 46:12-21; Dkt. 1597, Feb. 2023 Nakamura Decl. ¶ 50-51, Dkt. 1597, Feb. 2023 Nakamura Decl. Exs 10-12.

95. Dr. Gilbert was unaware of the study the SOS's Office commissioned confirming very low voter verification of ballots in Georgia 2020 elections and thus did not consider that study or its findings for his analyses and opinions. Opp. Ex. 95; Opp. Ex. 71 at 41:24-43:5.

96. Georgia election code mandates voting on devices that print "an elector verifiable paper ballot" and "produce paper ballots which are marked with the elector's choices in a format readable by the elector." O.C.G.A. § 21-2-2(7.1); O.C.G.A. § 21-2-300(a)(2).

97. The Dominion BMD system that Georgia currently uses does not accomplish the statutory mandate of producing paper ballots which are marked with the elector's choices in a format readable by the elector. Dkt. 1131, Halderman Report at ¶ 3.2; Opp. Ex. 57 ¶ 6; *see also* Opp. Ex. 91 at 82 (“[T]he evidence shows that the Dominion BMD system does not produce a voter-verifiable paper ballot or a paper ballot marked with the voter's choices in a format readable by the voter because the votes are tabulated solely from the unreadable QR code. Thus, under Georgia's mandatory voting system for ‘voting at the polls’ voters must cast a BMD-generated ballot tabulated using a computer-generated barcode that has the potential to contain information regarding their voter choices that does not match what they enter on the BMD (as reflected in the written text summary), or could cause a precinct scanner to improperly tabulate their votes.”).

98. Hand-marked paper ballots provide a reliable, software-independent record of the selections each voter actually made when registering their votes on the ballots, because there is no possibility whatsoever that a misconfiguration, a computer glitch, or malware will cause the voter's pen to handwrite a selection on the ballot the voter did not intend or actually make or otherwise alter the voter's

selections on the ballot itself. Opp. Ex. 87 at 62:6-15; Opp. Ex. 96; Opp. Ex. 92 at 2; Opp. Ex. 89 ¶ 4; Opp. Ex. 55 at 256:23-257:3.

99. Election officials also have options to help protect voters using hand-marked paper ballots from their own mistakes, such as configuring scanners to reject overvotes (where a voter registers more than one selection among the choices for a particular contest or question on the ballot) and to warn voters about undervotes, the most common kinds of voter errors (undervotes—where a voter does not register a selection for every contest or question on the ballot—are often intentional by voters rather than errors. Opp. Ex. 88 ¶ 27; Opp. Ex. 97 ¶ 44.

100. In 2020, numerous marks by voters on paper ballots erroneously were not detected by the Dominion scanning software and thus the ballots were not fully or properly tabulated, even though vote review panelists unanimously agreed on the candidate that the voter intended to select for affected contests, a fact that one vote review panelist found “truly disturbing.” Opp. Ex. 98.

101. Election security experts, including Defendants’ own election experts, recommend using HMPBs as the primary method of voting. Opp. Ex. 99 at PDF p. 165, ¶¶ 6, 15; Opp. Ex. 55 at 84:2-8, 91:4-15, 96:2-6; Opp. Ex. 92; Opp. Ex. 56 at

109:1-3, 135:23-136:2; Opp. Ex. 5 at 56-57; *see also* Opp. Ex. 100 (stating that his “ideal voting model is one where voters get to choose BMD or hand marked, where audits happen regularly, and where machines are maximally transparent and use modern security features”); Opp. Ex. 87 at 125:7-12; Opp. Ex. 92 at 2.

102. The vast majority of U.S. jurisdictions use hand-marked paper ballots (“HMPBs”) as the primary method of voting, with BMDs used only for voters who need or request them (e.g., those with certain disabilities). Dkt. 1131, Halderman Report at ¶ 2; Opp. Ex. 57 ¶ 6; Opp. Ex. 102; Opp. Ex. 103; *see also* Opp. Ex. 104 at 8.

103. The current consensus among election security experts is that BMDs, such as the Dominion ICX at issue, are not a secure method of voting due to fundamental flaws and that there is no known way of remedying those flaws other than to abandon BMDs except for those voters who cannot mark a paper ballot with a pen. Opp. Ex. 56 at 45:10-46:5; SMF Ex. 59 ¶¶ 5-6, 22-23, 25, 45, 77; Opp. Ex. 105 at 11:9-13:20, 271:4-272:6; Opp. Ex. 32; Opp. Ex. 33; Opp. Ex. 87 at 42:21-43:4; Dkt. 1589, Feb. 2, 2023 Stark Decl., ¶¶ 6-7, Ex. 5 at 2; Opp. Ex. 96.

104. In addition, the National Academies of Sciences, Engineering, and Medicine has found that there is no technical mechanism currently available that can ensure that a computer application used to record voter selections will produce accurate results; testing alone cannot ensure that systems have not been compromised; and any computer system used for elections – such as a voting machine or e-pollbook – can be rendered inoperable, which is why software-independence is critically important for voting systems that use any computer devices or applications. Opp. Ex. 3 at PDF p. 110; *see also* Opp. Ex. 91 at 25 (citing Opp. Ex. 3 at PDF p. 70, 108); *see also* Opp. Ex. 56 at 41:12-19; 110:5-21; SMF Ex. 59 ¶¶ 20, 30.

105. SOS CIO Merritt Beaver was not familiar with the well-recognized computer science concept of software independence. Opp. Ex. 31 at 133:7-11.

106. In 2018, the National Academy of Science noted that research on BMD verification was limited and warned against the specific style of BMD (with summary ballots) used in Georgia, stating that “[a]dditional research on ballots produced by BMDs will be necessary to understand the effectiveness of [BMD] ballots.” Opp. Ex. 3 at PDF p. 107-08. That additional research has led to the

current consensus against BMD systems like that used in Georgia for all in-person voters statewide as described above.

107. Numerous Georgia counties have had difficulties reconciling vote totals cast on the BMDs. *See, e.g.*, Opp. Ex. 106; Opp. Ex. 107; Opp. Ex. 108; Opp. Ex. 76; Opp. Ex. 109.

108. Defendants' expert Dr. Juan Gilbert has designed a new BMD for the very purpose of trying to remedy the well-recognized, serious deficiencies with BMDs like the Dominion BMDs Georgia uses. Opp. Ex. 110 ("BMDs. . .in voting machines are often nontransparent, hackable, and overly complex"); Opp. Ex. 71 at 55:11-20, 57:19-25.

109. Under the current BMD system, the threshold bottleneck during voter check-in significantly has contributed to long lines and waiting periods of hours (far greater than 30 minutes) and caused voters to leave and be deterred from voting. . . . combined with issues related to the power supply limitations at multiple polling places (causing equipment shutdowns), repeated issues with the operation of the PollPads and BMDs themselves, and ineffective or nonexistent 'non-technical' backup systems in place has led to a severe burden on the rights of

voters” Opp. Ex. 34 at 47, 49-50; Opp. Ex. 63 at 131:10-132:12, 134:19-138:16; Opp. Ex. 111; Opp. Ex. 112; Opp. Exs. 113-118.

110. In June 2020, multiple Georgia counties had to turn prospective voters away because BMDs were not working and the counties did not have paper ballots to offer. *See, e.g.*, Opp. Ex. 119; Opp. Ex. 120; Opp. Ex. 63 at 131:10-132:12; Opp. Ex. 111.

111. In 2019, Jennifer Doran, Election Supervisor for the Morgan County Board of Elections & Registration, was directed by her board to ask the Secretary of State whether Morgan County could conduct elections using hand-marked paper ballots, but the Secretary of State informed her that Morgan County could not use hand-marked paper ballots in any elections—notwithstanding that Georgia law affords county election superintendents discretion to adopt HMPBs when they deem the BMD system infeasible to use. Opp. Ex. 44 at 331:8-17; *see also* O.C.G.A. §§ 21-2-281, 21-2-334.

112. For absentee ballots that cannot be scanned in Georgia elections, election officials use BMDs to purportedly duplicate those ballots for tabulation purposes, which means that voters who vote by HMPB via Georgia’s absentee

system nonetheless may end up with their votes subject to Georgia's BMD system (without that information being disclosed to those voters, no less). Opp. Ex. 48 at 224:18-228:17; Dkt. 1593, Feb. 2023 Dufort Decl. ¶¶ 11-13, Ex. A.

113. Multiple SOS employees with responsibility related to the administration of Georgia elections were not aware that Logic and Accuracy testing is unlikely to detect malware. Opp. Ex. 48 at 38:1-24; Opp. Ex. 105 at 252:4-19.

114. Multiple SOS employees with responsibility related to the administration of Georgia elections or the SOS Office's IT systems were not aware that certain malware can defeat hash testing. Opp. Ex. 31 at 91:25-92:10; Opp. Ex. 48 at 38:1-24.

115. Michael Barnes believed that testing a single BMD and printer on election day was a reliable testing method, based on the fact that if one BMD shows proper operation, the others would as well. Opp. Ex. 105 at 27:20-29:3.

116. Parallel testing of a single voting machine, at best, will only reveal whether that particular machine has been infected with malware, and thus this sort

of parallel testing is not reliable for assessing the operation of voting machines beyond that one machine. Opp. Ex. 5 at 104:24-106:25.

117. State Defendants' expert, Dr. Michael Shamos, does not have confidence in a parallel testing procedure that only selects one machine out of some 27,000 for testing. Opp. Ex. 5 at 107:1-11.

118. There are technical implications for systems that are not adequately logic and accuracy tested, which could result in configuration problems not being caught, particularly if it is with the ballot-printing portion of the system. *See* Opp. Ex. 121 at 107:15-108:17, 129:24-130:10, 130:8-10, 130:15-21, 130:25-132:4 (Skoglund Testimony).

119. It is not sound cybersecurity practice to ignore known vulnerabilities simply because there may be other unknown vulnerabilities in an election system. Opp. Ex. 56 at 142:9-14.

120. That voters with disabilities may be vulnerable to BMD-hacking is not a reason to needlessly subject voters who can mark a paper ballot by hand to the risk of their votes being stolen by a hacked BMD. Opp. Ex. 93 ¶ 17.

121. Mr. Beaver said his team received reports from Georgia counties on a regular basis that someone in the office clicked on something that introduced malware onto the computer system. Opp. Ex. 31 at 164:25-167:8.

122. Mr. Barnes did not know who in the SOS Office would actually deal with security vulnerabilities. Opp. Ex. 105 at 98:5-100:24.

123. The SOS Office did not undertake any investigation for Curling Plaintiffs' interrogatories before responding to them that State Defendants were unaware of "any election equipment used with the Dominion election system being hacked in an election in Georgia." Opp. Ex. 48 at 171:17-177:7.

124. Curling Plaintiffs have repeatedly served interrogatories requesting information about *unauthorized access* to voting system components that State Defendants refused to answer at all or only evasively, such as only denying knowledge specifically of a hack. Opp. Ex. 122; Opp. Ex. 123.

125. After narrowing the requests in response to State Defendants' refusal to answer the interrogatories, State Defendants sent an unverified Word document from Vincent Russo denying that Georgia's election system had been hacked.

Opp. Ex. 124; Opp. Ex. 123 at Aug. 23, 2021 Response to Rog 15 & Oct. 21, 2021 Response to Revised Rog 15; Opp. Ex. 125.

126. Despite repeated requests for State Defendants to remedy the incomplete and evasive October 21, 2021 interrogatory responses and for a signed verification of those written responses, State Defendants refused to provide either, verifying only *other* interrogatory responses. Opp. Ex. 123 (verifying State Defendants October 1, 2021 responses, not the October 21, 2021 responses). Notably, State Defendants provided their evasive October 21, 2021 responses to Curling Plaintiffs' interrogatories asking about “each successful or *attempted* instance of unauthorized access to or copying or alteration of” any data on any component of Georgia’s BMD voting system just a few months after investigating a potential unauthorized access in Coffee County (in response to the Cyber Ninjas card James Barnes shared with the SOS Office in May 2021) and replacing the Coffee County EMS server and ICC due to a possible compromise, as James Barnes testified. *See* Opp. Ex. 123 at Oct. 21, 2021 Response to Revised Rog 15; Opp. Ex. 67 at 159:25-162:12; Opp. Ex. 127.

127. The State has not produced any evidence that any cybersecurity assessment of Georgia’s voting equipment, including its BMDs, printers, ICCs,

ICPs, and EMS servers, has been done. Opp. Ex. 69 at 106:25-108:2; Opp. Ex. 31 at 42:7-18; Opp. Ex. 105 at 227:2-25; Opp. Ex. 70 at 163:3-165:3; Opp. Ex. 54 ¶ 12.

128. Michael Barnes could not identify any cybersecurity election expert that has endorsed the current Georgia voting system as reliable, and does not know why the SOS has not arranged for one to examine the election system. Opp. Ex. 105 at 296:5-297:11.

129. James Oliver stated that if he had been at the SOS Office when it was made aware of the vulnerabilities with BMD machines, he would have recommended steps be taken to remedy the vulnerabilities. Opp. Ex. 30 at 140:22-141:2, 142:25-143:24, 146:3-10.

130. Mr. Oliver also stated that it did not surprise him that the SOS Office did not take any measure to mitigate the vulnerabilities based on his experience in his role there. Opp. Ex. 30 at 140:22-141:2, 142:25-143:24, 146:3-146:10.

131. SEB Member Mashburn and former SEB Member Le would not support the use of an election system that could be hacked in a few minutes by a voter in the voting booth. Opp. Ex. 128 at 23:16-25:7; Opp. Ex. 129 at 22:4-23:2.

132. SEB Member Mashburn and former SEB Member Le would not support the use of a system that could be hacked in a way that altered the QR code but not the human readable text of the ballot. Opp. Ex. 128 at 35:10-19; Opp. Ex. 129 at 27:10-29:10.

133. There is no evidence that anyone with technical expertise has presented to the SEB about how Georgia's BMD voting system works. Opp. Ex. 128 at 103:21-104:4; Opp. Ex. 130 at 45:14-46:12, 55:9-56:1.

F. The July 2021 Halderman Report Identified Numerous Serious Vulnerabilities with Georgia's Current BMD System.

134. Dr. Halderman is a renowned Professor of Computer Science and Engineering at the University of Michigan. This Court has accepted him as an election security expert. Opp. Ex. 2 at 23 n.19; Opp. Ex. 91 at 24 n.28.

135. Per a Court order, on September 4, 2020, Fulton County provided Dr. Halderman a BMD and an ImageCast precinct programmed with Dominion software. Opp. Ex. 91 at 24.

136. Dr. Halderman conducted extensive testing on the Fulton County BMD and related equipment and software over the course of 11 work sessions, including included examining the machines, testing for vulnerabilities, and developing proof of concept attacks. Dkt. 1131 at 4, 19.

137. Dr. Halderman discovered many serious vulnerabilities in the Georgia BMD provided by Fulton County that facilitate the introduction of malicious software, including malware that changes BMD QR codes and defeats Georgia's purported security tests of the equipment—namely, acceptance testing, logic and accuracy testing, and hash verification safeguards. Opp. Ex. 131 ¶¶ 6-9; Opp. Ex. 4 ¶¶ 48-49; *see also* Opp. Ex. 36 at 55:5-22 (Vincent Liu Testimony).

138. On July 1, 2021, Dr. Halderman produced a 26,000-word analysis of Georgia's BMD voting system, detailing numerous, serious cybersecurity vulnerabilities and the steps that a malicious actor could take to exploit these vulnerabilities to alter individual votes and election outcomes without detection,

including by introducing malware into the system through temporary physical access or remotely via the EMS server. Dkt. 1131, Halderman Report at 4-5.



139. After receiving the July 2021 Halderman report, State Defendants repeatedly insisted through at least late 2021 that the Court seal the report and treat it as Attorneys Eyes Only, thus confirming the highly sensitive nature of Dr. Halderman's findings and their serious implications for the insecurity and unreliability of Georgia's current BMD voting system. *See* Opp. Ex. 132. Dr. Halderman's report demonstrates that the vulnerabilities in Georgia's BMD voting system provide multiple routes by which attackers can install malicious software on Georgia's BMDs, either with temporary physical access or remotely from election management systems (EMSs). Dkt. 1131, Halderman Report at 5.

140. Dr. Halderman showed that—even without access to the BMD—an attacker can alter the QR codes a BMD prints on ballots to modify voters' selections. Dkt. 1131, Halderman Report at 20; Opp. Ex. 121 at 22:10-29:4; Opp. Ex. 133 (stillshots of Dr. Halderman's BMD printer prototype attack video); Opp. Ex. 134 (Side-by-side of Ballots from system hack); Opp. Ex. 135 (Scanner Results of Photocopied Ballots).

141. Dr. Halderman’s demonstration confirms the warnings Dr. Wenke Lee shared with the SOS and the S.A.F.E. Commission in 2018 and 2019. Opp. Ex. 92 at 4-5 (“Researchers already have demonstrated attack methods that can change votes recorded by a DRE or BMD. It requires no imagination to know that real attackers will try similar attacks on our election and voting systems.”).

142. Since September 2020, Dr. Halderman has continued his analysis of the BMD equipment and software and discovered additional serious vulnerabilities in the BMDs that facilitate the introduction of malicious software, including malware that changes BMD QR codes and defeats Georgia’s acceptance testing, logic and accuracy testing, and hash verification safeguards. Opp. Ex. 131 ¶¶ 6-9.

143. Contrary to the initial claims of State Defendants’ purported agent, Dominion, that its QR codes are encrypted (Opp. Ex. 136 at -612), Dr. Halderman showed that “ [REDACTED] ” and instead QR codes “ [REDACTED] ” [REDACTED] .”
Dkt. 1131, Halderman Report at 20; Opp. Ex. 36 at 55-56; Opp. Ex. 4 ¶¶ 37-40.

144. Dominion’s QR codes do not contain a unique identifier, thus, “
.” Dkt. 1131, Halderman Report at 23-24 (emphasis in original); Opp. Ex. 36 at 319:22-320:6; Opp. Ex. 4 ¶ 46.

145. The ICP scanners used in Georgia will tabulate ballots generated by a Georgia BMD and copied using a standard office photocopier or printer. Dkt. 1131, Halderman Report at 23; Opp. Ex. 36 at 82:15-21.

146. A genuine BMD ballot generated by Georgia’s BMD system may be copied and tabulated to stuff the ballot box. Dkt. 1131, Halderman Report at 23; Opp. Ex. 121 at 28:23-29:2.

147. Dr. Halderman’s July 2021 report identifies at least seven critical failings in Georgia’s current BMD system. Dkt. 1131, Halderman Report at 4-5.

148. Dr. Halderman found that critical vulnerabilities in the ICX BMD used in Georgia—and the wide variety of lesser but still serious security issues identified—indicate that it was developed without sufficient attention to security during design, software engineering, and testing, resulting in a “brittle” system

architecture that can be completely exploited by small mistakes. Dkt. 1131, Halderman Report at 7-8.

149. Some of the critical vulnerabilities Dr. Halderman identified in Georgia's ICX BMDs could be at least partially mitigated through changes to its software, but merely patching these specific problems is unlikely to make the ICX substantially more secure overall. Dkt. 1131, Halderman Report at 7.

150. A paper ballot generated from Georgia's ICX BMDs does not mitigate any security concerns with the equipment, because ICX malware can still change individual votes and election outcomes without detection. Dkt. 1131, Halderman Report at 7; Opp. Ex. 121 at 38:24-39:4.

151. The ICX BMDs used in Georgia have even more security risks than the predecessor DREs which this Court found were unconstitutionally insecure, because malware is easier to create for the ICX BMD system than for the DRE system. Dkt. 1131, Halderman Report at 34; Opp. Ex. 55 at 54:1-21; Opp. Ex. 131 ¶ 11; *see generally* Opp. Ex. 29.

152. Dr. Juan Gilbert, Defendants' own election expert, did not disagree with the many technical failings Dr. Halderman reported and even identified him as one of two election security experts he would rely on to assess the cybersecurity of voting equipment. Opp. Ex. 71 at 144:7-17, 216-45.

153. Secretary Raffensperger repeatedly dismissed Dr. Halderman's findings with the unsupported claim that his access to Georgia's voting equipment could not be replicated by a real-world bad actor—a claim vitiated at least by the 2021 Coffee County breach. Opp. Ex. 137; *see, infra*, Section K.

154. Secretary Raffensperger misleadingly criticized Dr. Halderman's analyses on the basis that he received certain information to access the Dominion voting equipment, despite the fact Dr. Halderman's report itself rebuts this claim, and the SOS's Chief Information Officer and Rule 30(b)(6) deponent admitted that it is standard practice to receive such information for cybersecurity assessments. Opp. Ex. 137 at 13-14; Dkt. 1131, Halderman Report at 33, 39, 44-45; Opp. Ex. 138 at 271:2-273:17, 396:13-397:11; Opp. Ex. 32; Opp. Ex. 33.

155. Gabriel Sterling was aware in or around the fall of 2020 that Dr. Halderman was able to hack the QR code on a Georgia BMD as demonstrated for the Court at that time. Opp. Ex. 48 at 68:17-72:7.

156. It is possible to design fraudulent software that could self-propagate to multiple BMDs used throughout Georgia and that would be adaptable to multiple ballot styles. Opp. Ex. 56 at 85:3-16; 85:22-86:12, 86:13-87:11, 99:3-100:8, 101:3-6.

157. On January 27, 2022, Secretary Raffensperger publicly asked Dr. Halderman to request that this Court release his report, a request Dr. Halderman and Plaintiffs already had made multiple times and which State Defendants had opposed each time. *See* Opp. Ex. 139.

158. A voting system that uses a barcode on a paper ballot as the exclusive means of interpreting the voter's choices increases the likelihood that attackers will be able to compromise election results, because the use of barcodes makes it possible for attackers to commit difficult-to-detect fraud by hacking either the scanners or the BMDs. Opp. Ex. 57 ¶ 5.

159. Producing an entirely human-readable ballot that uses the human-readable text for tabulation rather than a barcode that is not human-readable, if deployed in Georgia, would somewhat mitigate—though not eliminate—the risk of hacking Georgia’s BMDs because voters then could at least verify the portion of their ballots that would be tabulated, though unfortunately few voters actually do that in practice. Opp. Ex. 57 ¶ 11.

160. The kinds of attacks that Dr. Halderman demonstrated on the Dominion BMDs—attacks that replace the software running in the ICX and make arbitrary changes to the ballots that it prints—are the most serious kind of attack that you could have on voting equipment. Opp. Ex. 55 at 46:25-47:8, 182:2-11.

161. For a voting system with HMPBs tabulated with optical scanners paired with rigorous audits, the primary method of attack would be retail-level tampering with single pieces of paper at a time, which is *much more* difficult to do at a wide scale than the kinds of electronic fraud that can be used to attack Georgia’s BMD voting system. Opp. Ex. 55 at 28:18-29:5.

162. Dr. Halderman’s findings regarding the security vulnerabilities of the BMD system used in Georgia may reasonably leave Georgia voters with

diminished confidence that the votes they cast on ICX BMDs will be counted correctly, or that any future elections conducted using Georgia's BMD system will be reasonably secure from attack. Dkt. 1131, Halderman Report at 8; *see also* Opp. Ex. 55 at 76:4-15, 259:20-260:24; Opp. Ex. 264 at 37:7-17, 43:21-44:11.

163. Neither the SOS Office's Chief Information Officer (Merritt Beaver), Chief Operations Officer (Gabriel Sterling), Director of the Center for Election Systems (Michael Barnes), Security Manager (James Oliver), nor Chief Information Security Officer (David Hamilton) had read Dr. Halderman's July 2021 report at the time of their depositions and thus were unable to address his many serious findings, despite their responsibility related to Georgia's elections or the SOS Office's IT systems. Opp. Ex. 69 at 183:4-184:12, 189:5-193:22, 201:12-21; Opp. Ex. 48 at 21:15-24:12; 26:15-28:24; Opp. Ex. 85 at 74:15-78:6; Opp. Ex. 30 at 140:22-141:2, 142:25-143:24, 146:3-10; Opp. Ex. 105 at 96:15-97:19; Opp. Ex. 128 at 53:15-54:14; 57:9-18.

164. All but one current and former SEB member who were asked had not read Dr. Halderman's July 2021 report at the time of their depositions and thus were unable to address his many serious findings, despite their responsibility related to Georgia's elections. Opp. Ex. 140 at 14:18-15:9; Opp. Ex. 129 at 51:16-

57:17; Opp. Ex. 141 at 53:1-21, 55:19-23; Opp. Ex. 130 at 50:11-24, 52:13; Opp. Ex. 63 at 72:12-16; 72:21-25, 94:12-20, 97:20-98:12; Opp. Ex. 142 at 9:20-10:7.

165. The single SEB member who had read Dr. Halderman's July 2021 report admitted that it raised questions regarding the vulnerabilities in the BMD systems—for which that SEB member had no answers or solutions, despite his responsibility related to Georgia's elections. Opp. Ex. 142 at 11:12-19.

166. Michael Barnes did not know why the SOS Office decided not to share Dr. Halderman's findings regarding security failings with Georgia's BMD system with him and others, despite their responsibility related to Georgia's elections. Opp. Ex. 105 at 96:15-97:19.

167. As the CISO, David Hamilton would expect to have been made aware of Dr. Halderman's testimony that he was able to hack Georgia's BMD equipment in *only three* days and that is something Mr. Hamilton would have liked to have known about—but he did not know. Opp. Ex. 69 at 183:4-184:12, 189:5-193:22, 201:12-21.

168. Defendants have offered no evidence that they have taken steps to remediate the many serious vulnerabilities identified by Dr. Halderman with Georgia’s BMD system, despite their unsupported public claims that “Georgia’s election system is safe and secure.” Opp. Ex. 69 at 193:24-198:17; Opp. Ex. 105 at 98:5-100:24; Opp. Ex. 85 at 74:15-78:6; Opp. Ex. 48 at 68:17-72:7; Opp. Ex. 63 at 72:12-16; 72:21-25, 94:12-20, 97:20-98:12, 100:21-25, 101:1-6; Opp. Ex. 138 at 373:3-376:22; Opp. Ex. 139 (“Sensationalized media articles and misleading reports from paid activists notwithstanding, Georgia’s election system is safe and secure.”).

169. When asked who within the SOS Office would have responsibility for ensuring that security vulnerabilities with Georgia’s voting equipment were remediated, Mr. Hamilton testified probably the CISO, which was his role at SOS Office—and yet he was not informed of the security vulnerabilities Dr. Halderman found with the equipment, including those demonstrated for the Court during the September 2020 preliminary injunction hearing. Opp. Ex. 69 at 193:24-198:17.

G. An Independent Government Cybersecurity Agency Verified Dr. Halderman’s Findings and Recommended Mitigation Measures.

170. On January 21, 2022, the Cybersecurity and Infrastructure Security Agency (“CISA”) within the Department of Homeland Security agreed to conduct

an analysis of Georgia’s BMD system with the condition that its findings would likely need to be shared with “affected end users” of the Dominion BMD system subsequent to the application of appropriate mitigation measures. Opp. Ex. 143.

171. On February 2, 2022, this Court authorized Dr. Halderman to share his July 2021 report with CISA. Opp. Ex. 144 at 2.

172. CISA notified the Court that it had commenced analyzing the Georgia BMD system using its standard Coordinated Vulnerability Disclosure (“CVD”) process on February 10, 2022. Opp. Ex. 144 at 2.

173. Between February and June 2022, CISA completed the CVD process, working closely with Dr. Halderman and Dominion Voting Systems and coordinating with relevant stakeholders. Opp. Ex. 145 at 1.

174. As a result of its CVD process CISA released a public advisory corroborating the July 2021 Halderman Report findings and detailing nine serious vulnerabilities in Georgia’s BMD system. Opp. Ex. 146 §§ 2.2.1-5, 2.2.7, 2.2.9.²

175. Among these nine serious vulnerabilities, CISA confirmed the QR code vulnerability described in Dr. Halderman’s July 2021 report, noting that the “authentication mechanism” voters are required to use to vote on the BMD device “is susceptible to forgery,” and that “[a]n attacker could leverage [the QR code] vulnerability to print an arbitrary number of ballots without authorization.” Opp. Ex. 146 § 2.2.9. In the first release of its Advisory that went to secretaries of state across the U.S., CISA advised against the use of the QR code option with Dominion’s BMD system. Opp. Ex. 146 § 3 (“[J]urisdictions should, where

² The CISA Advisory constitutes public findings resulting from CISA’s Coordinated Vulnerability Disclosure process, which analyzed vulnerabilities in Georgia’s Dominion voting system as identified in the July 2021 Halderman Report. Opp. Exs. 147, 148. The CISA Advisory is thus admissible under the public records exception to the rule against hearsay, and Plaintiffs are entitled to rely on it. Fed. R. Evid. 803(8); *see Crawford v. ITW Food Equip. Grp. LLC.*, 977 F.3d 1331, 1348-49 (11th Cir. 2020) (finding OSHA reports admissible under the public records exception to the hearsay rule because they were factual findings from a legally authorized investigation and noting the hearsay rule’s underlying policy of broad admissibility of public records containing evaluative conclusions because such reports are presumptively reliable).

possible, configure the ImageCast X to produce traditional, full-face ballots, rather than summary ballots with QR codes.”)

176. The CISA Advisory described several methods an attacker could use to introduce malicious code to the BMD system via removable media or remotely from the EMS server. Opp. Ex. 146 § 2.2.1, § 2.2.3, § 2.2.4, § 2.2.5, § 2.2.7.

177. The CISA Advisory recommends 13 steps for Georgia to mitigate the risk that bad actors could exploit the vulnerabilities. Those steps include three physical security measures, seven cybersecurity measures, and three recommendations related to ballot verification, post-election testing and audits. Opp. Ex. 146 § 3.

178. Gabriel Sterling agreed that the vulnerabilities identified by CISA should be mitigated as CISA advised. Opp. Ex. 149 at 11:12-13:22, 349:16-21; Opp. Ex. 32; Opp. Ex. 33; *see also* Opp. Ex. 105 at 98:5-100:24.

179. Defendants have offered no evidence indicating that any of the 13 mitigation steps recommended by CISA have been implemented in Georgia. *See,*

e.g., Opp. Ex. 142 at 21:6-24:1; Opp. Ex. 150 at 176:25-177:22; Opp. Ex. 151 at 167:4-18; Opp. Ex. 138 at 373:3-376:22.

H. Defendants' Experts Never Examined Georgia's Voting Equipment and Admit Key Vulnerabilities.

180. State Defendants' expert, Dr. Michael Shamos, confirmed many serious failings with Georgia's DRE/GEMS system that rendered it unconstitutional and advised against barcode BMDs like those used in Georgia. Opp. Ex. 5 at 56:13-57:21.

181. Dr. Wenke Lee, whom then-Secretary and current-Governor Brian Kemp selected as the sole election cybersecurity expert on the Georgia's SAFE Commission, objected to the use of BMDs in Georgia. Opp. Ex. 152 at 4; Opp. Ex. 92 at 2-3.

182. In a reference document created for the SAFE Commissioners, Dr. Lee stated that "[a] secure voting system should use hand-marked paper ballots instead of ballot marking devices. . . . This consensus approach among the cybersecurity research community ensures that votes by the voters are counted accurately." Opp. Ex. 152 at 4.

183. In an addendum to the reference document created for the SAFE Commissioners, Dr. Lee stated that “[a] voting system must provide either a human readable, post-vote paper receipt from a ballot-marking device or an actual paper ballot as the durable, independent evidence that can be used as the authoritative source document in an audit or recount.” Opp. Ex. 92 at 2.

184. Dr. Eric Coomer retained Dr. Halderman as his own election security expert regarding Dominion’s BMDs. Opp. Ex. 55 at 10:1-6; Opp. Ex. 153.

185. Dr. Ben Adida, Defendants’ audit expert, has not testified or submitted additional opinions in this matter since the 2020 preliminary injunction hearing. Opp. Ex. 36.

186. None of Defendants’ experts have conducted cybersecurity examinations of Georgia’s Dominion voting equipment. Opp. Ex. 71 at 13:12-17, 68:4-22; Opp. Ex. 5 at 84:24-86:8.

187. Dr. Gilbert was unaware that Fortalice found serious cybersecurity vulnerabilities with the SOS Office’s IT systems and thus did not consider that information for his analyses or opinions in this case. Opp. Ex. 71 at 269:11-23.

188. Dr. Gilbert was not aware that Georgia's previous DRE/GEMS system had not actually been "air gapped" as State Defendants claimed (it had been connected to phone lines, via a modem, and used with removable media that also had it been used with internet-connected computers), and thus he did not consider that information for his analyses or opinions in this case. Opp. Ex. 71 at 267:10-21.

189. Dr. Gilbert was not aware that removable media used with Georgia's previous DRE/GEMS system may have been reused with the Georgia's new BMD system, and thus did not consider that information for his analyses or opinions in this case. Opp. Ex. 71 at 213:3-216:19.

190. Dr. Gilbert agreed that Dr. Halderman had identified numerous attacks that could be readily implemented against Georgia's BMD system, including manipulation of QR codes or human-readable text, and did not disagree with Dr. Halderman's findings regarding the manner and ease with which those attacks could be effected in Georgia. Opp. Ex. 71 at 74:19-22, 105-09, 186:4-208:9, 216:20-245:22.

191. Dr. Gilbert did not dispute that, in contrast, altering hand marked paper ballots requires many hours to manually change ballots— and any alteration to a hand-marked paper ballot could occur only after *the ballot is tabulated by the scanner*. Opp. Ex. 71 at 134-35.

192. Dr. Gilbert testified that he is not a cybersecurity expert and thus lacks the expertise to evaluate the cybersecurity of Georgia’s voting system. Opp. Ex. 71 at 143-44.

193. Dr. Gilbert admitted that eliminating QR codes “would get rid of a lot of the issues” Dr. Halderman found with Georgia’s BMD system, and “recommend[ed] not using [QR codes] to eliminate all these discussions and concerns around them.” Opp. Ex. 71 at 89:7-13, 90:9-16.

I. Defendants’ Own Cybersecurity Consultant Identified Vulnerabilities.

194. The SOS Office retained a cybersecurity consulting company, Fortalice Technical Solutions, to identify weaknesses in the SOS Office’s IT network and externally facing environment. Fortalice’s role was to review the infrastructure and make recommendations as to what should be improved and

identify weaknesses that needed to be strengthened. Opp. Ex. 154 at 5-6; Opp. Ex. 30 at 65:11-23.

195. Theresa Payton, CEO and Chief Advisor for Fortalice Solutions, and certain of her colleagues at Fortalice, found serious security failings with the SOS Office's IT networks and opined that it is only a matter of time until a U.S. election is hacked. Opp. Ex. 154 at 5-6; Opp. Ex. 37; Opp. Ex. 38; Opp. Ex. 155; Opp. Ex. 29 at 219:11-23, 225:1-226:4, 227:22-228:19.

196. In Fortalice's assessment in October of 2017, Fortalice identified 22 security risks in the networks that they examined, characterizing most of those risks as significant. Opp. Ex. 29 at 29:16-30:2, 219:11-16.

197. One of the significant risks that Fortalice identified in the 2017 risk assessment was widespread local administrative rights, which granted every Georgia SOS Office employee administrative rights on their workstations and every other work station in the SOS Office, and, thus, allowed every single user the ability to download software, affect the programming of that computer, and, ultimately, created a significant risk of malware infecting the election-related network. Opp. Ex. 29 at 32:15-33:23, 219:17-220:21.

198. Another vulnerability that Fortalice identified in the October 2017 risk assessment was that the SOS Office IT network relied on legacy systems and software that were no longer supported or receiving security patches even when new vulnerabilities were identified, which created a significant risk that a hacker could easily exploit the unpatched devices. Opp. Ex. 29 at 34:8-17.

199. Fortalice was able to penetrate aspects of the SOS Office IT network during the 2017 assessment, which allowed them to obtain domain administrator rights on the network they penetrated, gain access to the network security systems, and review the enterprise architecture and system configurations. Opp. Ex. 29 at 44:13-45:24.

200. The Fortalice team assessed the SOS Office IT security as Tier 2 on the NIST scale in the October 2017 assessment, which meant that “they had an awareness of cybersecurity risks at the organizational level but an organization-wide approach to managing cybersecurity risks had not been established.” Opp. Ex. 29 at 218:21-219:10.

201. The risk of nonunique local administrator passwords for the SOS Office IT network that were identified and recommended to be fixed in the October

2017 Fortalice assessment was still present in a November 2018 assessment by Fortalice. Opp. Ex. 29 at 223:11-25.

202. During the February 2018 assessment, Ms. Payton identified several missing critical operating system patches, unsupported software, and vulnerable third-party software with the SOS Office IT network. Opp. Ex. 29 at 227:6-9.

203. Fortalice's February 2018 assessment of the SOS Office IT network also identified 15 security risks involving PCC, the company who owned and operated the voter registration database at that time, and recommended those risks for remediation. The risks included that PCC was relying on outdated software that was known to contain critical security vulnerabilities which could be exploited by an attacker with sufficient time and resources, and that PCC was not blocking VPN connections from IP addresses of known threat sources or foreign countries. Opp. Ex. 29 at 225:1-25, 226:19-227:5.

204. The Fortalice team interviewed Chris Harvey during these assessments, who indicated that the voter registration databases is what Russian hackers would want to get into. Opp. Ex. 29 at 234:1-235:8.

205. Chris Harvey subsequently indicated to Fortalice that the PCC and the voter registration database was out of scope for the next Fortalice assessment in November 2018. Opp. Ex. 29 at 234:1-235:8.

206. Fortalice's November 2018 assessment resulted in 20 additional recommendations to the SOS Office IT network to improve their cybersecurity. Opp. Ex. 29 at 227:22-25.

207. As of the November 2018 assessment of the SOS Office IT network, weeks after the midterm election, 19 out of the 22 vulnerabilities identified by Fortalice in 2017 had not been remediated, and the SOS Office earned a numerical score of only *53.98 out of 100* from Fortalice. Opp. Ex. 29 at 228:14-17, 230:1-231:14.

208. The SOS Office's engagement for the three Fortalice assessments in 2017 and 2018 did not include examining GEMS servers, DREs, memory cards, and scanners; nor was Teresa Payton engaged to do that analysis for her declaration. Opp. Ex. 29 at 216:5-217:18.

209. Fortalice’s most recent Technical Assessment of the SOS Office IT network identified eight separate vulnerabilities, including four “High” risks, meaning that the vulnerability could be [REDACTED]

[REDACTED]
[REDACTED].” Opp. Ex. 154 at 5.

210. Neither Fortalice— nor anyone else— was asked to determine whether any of the vulnerabilities it identified with the SOS Office IT network or any other systems or equipment it examined at the SOS Office’s direction had been exploited by any outside party. Opp. Ex. 138 at 282:22-284:1.

211. The “High” level risks in the 2021 Fortalice Technical Assessment of the SOS Office IT network include directory traversal vulnerability (“ [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].”); insecure file shares; insecure password storage; and

weak passwords. Opp. Ex. 154 at 6-15.

212. Regarding insecure password storage, the 2021 Fortalice Technical Assessment found that many SOS Office employees appeared to be using Excel spreadsheets and Word documents for password storage. Opp. Ex. 154 at 14.

213. A Fortalice Report on “Web Vulnerability Remediation Checks” dated July 14, 2020 found that two remediation attempts by the SOS Office to fix vulnerabilities in the My Voter Page web application were unsuccessful. Opp. Ex. 156 at 2-3; Opp. Ex. 69 at 159:9-165:5. The vulnerabilities in the My Voter Page web application involved cross-site scripting and insecure direct object reference. Regarding insecure direct object reference, the Fortalice report found that unauthorized users could view precinct cards *belonging to other users*. Opp. Ex. 156 at 2-3.

214. A draft Fortalice Technical Assessment from May 2020 for the SOS Office IT network reported the findings of a penetration test from the perspective of a remote worker, which revealed several critical and high-risk vulnerabilities in the IT infrastructure, including two entirely separate routes to gain *administrative control of the entire SOS Office network*. Opp. Ex. 157; Opp. Ex. 69 at 62:5-64:20.

each of which bears critical responsibility for securing and maintaining many essential components of Georgia's voting system, including 159 EMS servers, tens of thousands of BMDs and printers, many ICC and ICP scanners, and much more. Opp. Ex. 29 at 275:25-276:7. Defendants have offered no evidence of any cybersecurity assessment of any aspect of Georgia's voting system conducted for, by, at the behest of, or in any of Georgia's 159 counties.

218. After this Court issued its preliminary injunction Order in August 2019 relying in part on certain Fortalice reports finding serious security failings with the SOS Office IT network, the SOS Office directed Fortalice to stop sending written reports of cybersecurity assessments to the SOS Office because, purportedly, "they were taken out of context by the public." Opp. Ex. 31 at 75:4-9, 159:16-24; Opp. Ex. 138 at 312:15-314:19, 331:17-22.

219. Now the SOS Office does conference calls with Fortalice to discuss assessments rather than obtain written reports memorializing their findings. Opp. Ex. 31 at 71:18-72:23. Plaintiffs obtained Fortalice cybersecurity assessment reports prepared after this Court's August 2019 preliminary injunction Order from Fortalice itself (over State Defendants' objections). Opp. Ex. 159.

220. No significant findings from the 2020 and 2021 annual assessments done by Fortalice for the SOS Office IT network were raised to Merritt Beaver, the SOS Office longstanding CIO. Opp. Ex. 31 at 71, 80:18-81:17; 83:4-84:4.

221. While Mr. Hamilton, the SOS Office former CISO, agreed with Fortalice's recommendations—many of which involved no cost to the SOS Office—and pushed the SOS Office to move faster on the recommendations, the SOS Office reportedly did not have enough people with enough training to make more headway on Fortalice's recommendations. Opp. Ex. 69 at 45:10-61:12.

222. Mr. Hamilton recommended that the SOS Office hire a full-time, permanent CISO, which would have been preferable to his fractional arrangement, but that recommendation was not adopted. Opp. Ex. 69 at 23:25-27:5, 35:5-36:13.

223. When Mr. Hamilton was planning to leave his position as CISO at the SOS Office, he reached out to Fortalice to tell them he would be leaving and to try to get their help in addressing a “backlog of security issues,” saying “there was definitely work to be done” and the SOS Office “needed some help”—but there is no evidence that backlog was resolved or that Fortalice or anyone else provided the necessary help. Opp. Ex. 69 at 68:13-70:9.

J. Georgia’s Election System Lacks Sufficient Safeguards to Protect Against Demonstrated Cybersecurity Vulnerabilities.

224. The SOS Office emphasized that “Physical security is . . . the front line of all cybersecurity.” Opp. Ex. 48 at 250:19-15.

225. During a hearing before the Congressional Committee on House Administration, Georgia’s Director of Election Administration, Kathy Rogers, testified: “The first line of security defense in any system is physical security. All other security measures go for naught if you leave the doors unlocked.” Opp. Ex. 9 at 110.

226. When asked who is responsible for the security of Georgia’s voting equipment, including knowing whether counties were reusing removeable media devices, the SOS Office said that the counties were, and that the counties are supposed to coordinate with CISA to check the security of voting equipment, including physical security, at the county level. Opp. Ex. 48 Feb. 24, 2022 SOS 30b6 (Sterling) Dep., at 118:1-120:8; Opp. Ex. 85SOS 30b6 (Harvey) Dep. at 105:15-25, 146:22-25; Opp. Ex. 105Feb. 11, 2022 SOS 30b6 (M. Barnes) Dep. at 30:22-31:1. Fulton County described how it “took a lot for [Fulton County] to get the State to produce any kind of poll worker manual” on the BMD system and how

“the State was pretty hands-off when it came to the system.” Opp. Ex. 70 at 58:14-59:16.

227. Regulations require that voting machine discrepancies, for example a broken seal or another concerns, need to be resolved *before* use, and BMDs found unsealed before an election should *not* be used. Opp. Ex. 31 at 49:5-51:7; 141:7-146:11; Opp. Ex. 85 at 54:25-55:17.

228. Secretary Raffensperger testified to a House Committee that because machines “always. . . have security, you know, tape on it, you know, so that you know that, if you broke it, broke the seal, that someone could’ve been in there,” and that “there was never any evidence of that that we are aware of.” Opp. Ex. 77 at 60. But this was not accurate, as the SOS Office was in fact aware of such evidence as described below.

229. Fulton County election workers used BMDs for the November 2020 election that, in violation of election policies, were found with the side doors of the voting machines that cover the machines’ removable media ports open, unsealed, and unsecured. Opp. Ex. 160; Opp. Ex. 85 at 50:3-15, 52:11-53:19, 54.25-56:1; Opp. Ex. 161 at Slide 12.

230. There is no evidence that an investigation occurred or that the Fulton County BMDs were tested for compromise or removed from future use, despite the fact that an election worker reported the incident to the SOS's Office with a complaint containing photo evidence of the unlocked machines in question. Opp. Ex. 160; Opp. Ex. 162; Opp. Ex. 85 at 50:9-15, 55:18-23.

231. A presentation on Fulton County "Election Day Issues," mentions that there was no seal on a scanner, in addition to other problems with BMDs, such as failure to power on, need to be reset, error signals, and other problems. Opp. Ex. 161 at Slide 6, 8.

232. The presentation also mentions how "Not enough seals [were] provided" on election day. Opp. Ex. 161 at Slide 10. The presentation specifically states that the Messiah Precinct did not have the required seal on the voting scanner. Opp. Ex. 161 at Slide 12.

233. Michael Barnes told multiple county elections supervisors to use BMDs for voting even though the BMD's seals had been removed or were missing. Opp. Ex. 163; Opp. Ex. 164.

234. There are multiple places where access to voting machines might be obtained in order to hack voting machines other than election warehouses, such as when the machines are being transported to polling places, when they are in polling places before or after an election, or when they are being transported from the polling places. Opp. Ex. 56 at 104:24-105:17.

235. Security at election warehouses is not always effective. Opp. Ex. 56 at 104:19-23.

236. Infiltration of hardware stored in an unlocked area could be easily accomplished simply by plugging in a USB drive containing malicious code. *See* Dkt. 1131, Halderman Report at 48; Opp. Ex. 146 § 2.2.1, § 2.2.3, § 2.2.4, § 2.2.5, § 2.2.7.

237. In Hart County, “many voting machines were left unlocked” during the day while the polls were open for the November 2020 election. Although the SOS’s Office learned about this issue, there is no evidence it was ever investigated. Opp. Ex. 162; Opp. Ex. 85 at 62:16-20.

238. In Fulton County during the November 2020 election, a scanner containing 400-500 ballots was left unsecured overnight, and the precinct's election manager did not report the ballots to Fulton County. Opp. Ex. 60.

239. Later that night, the election manager stopped at her house to take a shower in the middle of transmitting completed ballots, leaving them unsecured in her personal vehicle for nearly 20 minutes. Opp. Ex. 85 at 218:5-219:6; Opp. Ex. 60.

240. Although known to the SOS, there is no evidence of any investigation of the incident involving the election manager who left ballots unsecured in her vehicle, including whether the election tabulation in Fulton County was affected. Opp. Ex. 85 at 218:21-219:6.

241. In one Fulton County warehouse, election workers often left the storage area for the EMS server unlocked. Opp. Ex. 166 at 59:23-61:7.

242. One Fulton County pollworker reported that Dominion, not Fulton County Election Employees, seemed to be running an election warehouse, and that

people were opening up 40-50 standalone scanners and “emptying the ballots into suitcases,” with “no formal procedure.” Opp. Ex. 168.

243. U.S. and Georgia elections are targets of hackers seeking to disrupt the voting process. Opp. Ex. 29 at 205:20-206:12 (Payton testimony); Opp. Ex. 1 ¶¶ 8-12, Exs. B-G (PDF p. 47-76); *see also* Opp. Ex. 2 at 40-42; Opp. Ex. 52 at 1, 3, 5, 7, 9, 11-38.

244. In the 2022 midterm elections, the federal government renewed warnings that bad actors are working to compromise elections in the United States. *See* Opp. Ex. 169 (“The ability of persons located, in whole or in substantial part, outside the United States to interfere in or undermine public confidence in United States elections, including through the unauthorized accessing of election and campaign infrastructure or the covert distribution of propaganda and disinformation, continues to pose an unusual and extraordinary threat to the national security and foreign policy of the United States.”).

245. Fulton County experienced someone attempting to run vulnerability scans and run scripts to gain access into its external server environment, an

incident which Fulton County was concerned may have been a “politically motivated attack.” Opp. Ex. 170.

246. The SOS Office received a hacking threat via e-mail that stated: “

[REDACTED]

[REDACTED]

[REDACTED].” Opp. Ex. 171.

247. The usual process to deliver poll pads to poll managers is “just to hand them [poll pads] out on Sundays” before elections. In Fulton County, poll managers would even “put them [poll pads] in their cars” after receiving them from the county. Opp. Ex. 70 at 47:3-15.

248. This process of handing out poll pads on Sundays to poll managers is common among Georgia counties. Opp. Ex. 70 at 47:16-20.

249. Poll pads are internet-connected and can be used to watch Netflix, for example. Opp. Ex. 172 at 19; Opp. Ex. 173 at 49:22-50:11; Opp. Ex. 151 at 120:2-121:6.

250. The Coffee County EMS computer and ICC tabulation computer had Windows game applications installed. Opp. Ex. 172 at 20; Opp. Ex. 173 at 50:15-52:9; Opp. Ex. 151 at 121:7-122:6.

K. The Coffee County Breach Reveals the Lack of Meaningful Safeguards to Protect Georgia’s Voting System.

1. Election Officials in Coffee County Permitted Unauthorized Individuals Access to Georgia’s Election System

251. Dominion’s Contract with SOS Office defines a “Security Breach” as: “(i) unauthorized physical or technical access to any Contractor Computer System; (ii) any circumstance that may constitute or result in, any unlawful or unauthorized acquisition, access, loss, theft, use or disclosure of any Confidential Information, Regulated Information, or State Data in the possession of any of the Contractor Parties; (iii) any breach or attempted breach of the security of any Confidential Information, Regulated Information, or State Data, or of any of the controls of any of the Contractor Parties intended to protect the same; or (iv)) any other circumstances or events that could compromise the privacy or security of any of the Confidential Information, Regulated Information, or State Data in the possession of any of the Contractor Parties.” Opp. Ex. 84 at 45-46.

252. In January 2021, an infiltration of Georgia's voting system by a team from Atlanta-based forensics firm SullivanStrickler ("SS") was orchestrated by, *inter alia*, Coffee County Republican Party Chair Cathy Latham, bail bondsman Scott Hall, and Cyber Ninjas CEO Doug Logan, and local Coffee County election officials Misty Hampton and Coffee County Elections Board member Eric Chaney, who facilitated the SS team's entry into the elections office. Opp. Ex. 174; Opp. Ex. 175 at 18:19-19:3, 48:1-5, 111:7-9, 114:3-117:11, 114:12-147:5; Opp. Ex. 176; Opp. Ex. 177; Opp. Ex. 149 at 147:10-15; Opp. Ex. 263.

253. An organization founded and operated by Sidney Powell (an attorney for the Trump Campaign and for Cathy Latham) paid for the infiltration. Opp. Ex. 175 at 75:3-6; Opp. Ex. 178; Opp. Ex. 180 at 2.

254. Both testimony by SS and security video from the Coffee County elections office confirm the activity and movements of the forensics team, the coordination with Coffee County elections officials, and other facilitators, including Misty Hampton's assistant, Jil Ridlehoover, Hampton's daughter, and her daughter's boyfriend. Opp. Ex. 175 at 114:3-117:11, 144:12-147:5; Opp. Ex. 176.

255. On January 7, 2021, SS forensically imaged many components of Georgia's voting system *in its operational environment* in Coffee County, including the ICC, the EMS server, one or more pollpads, ICPs, a Dominion-supplied laptop, and extensive removable media, including one containing the Dominion ICX BMD software. Opp. Ex. 175 at 144:12-147:5, 290:7-14, 302:2-9; Opp. Ex. 75 ¶ 12.

256. The SS team made these copies at the direction and oversight of Latham, Chaney, Hall, and Hampton, in part by connecting various devices, including computers, to the voting equipment; some of the devices the SS team brought with them, exposing Georgia's operational voting system and its key components to potentially-compromised outside devices and software. Opp. Ex. 175 at 144:12-147:5; *see also* Opp. Ex. 75 ¶ 10.

257. The SS team made copies of software and other files, including Dominion's proprietary Democracy Suite software and actual election data, from the Georgia voting equipment and other devices in Coffee County. Opp. Ex. 175 at 144:12-147:5.

258. The SS team also collected scanned cast ballot images from actual Georgia elections and removable media provided to them by former Coffee County elections supervisor Misty Hampton. Opp. Ex. 175 at 290:7-14.

259. SS also attempted to image a Georgia BMD using a Cellebrite forensic extraction device, and succeeded in copying the Dominion BMD system installation software used in Georgia from a flash drive located in the Coffee County election office. Opp. Ex. 175 at 302:2-9; *see also* Opp. Ex. 75 ¶ 12.

260. SS did not use write-blocking equipment, as is industry best practice, to prevent the inadvertent transfer of data—such as malicious code—to the voting equipment. Opp. Ex. 181 at 38:8-25; *see also* Opp. Ex. 255 ¶¶ 30-31.

261. Evidence indicates that SS altered data on at least the Coffee County EMS server. Opp. Ex. 181 at 40:18-41:4; *see also* Opp. Ex. 255 ¶¶ 30-31.

262. From January 18-19, 2021, Doug Logan and Jeffrey Lenberg, a computer security consultant who has also analyzed Dominion voting equipment in Michigan in connection with efforts to discredit the 2020 Presidential election, visited the Coffee County elections office and spent significant time in the access-

restricted GEMS room and conducted a series of experiments on Georgia's voting equipment *in its operational environment*. Opp. Ex. 182; Opp. Ex. 183; Opp. Ex. 184 at 16:10-14; *see also* Opp. Ex. 75 ¶¶ 17-18.

263. During Mr. Logan and Mr. Lenberg's visits to Coffee County's elections office and access to Georgia's voting equipment *in its operational environment*, system dates on several election computers were altered, scanner settings were reconfigured several times, over 6,400 ballots were scanned, and one precinct scanner was physically opened to inspect the internal parts. Opp. Ex. 184 at 116-119, 122-130; *see also* Opp. Ex. 255 ¶ 9; Opp. Ex. 75 ¶ 18.

264. Mr. Lenberg returned to the Coffee County elections office, including the highly-restricted EMS server room, for five more days later in January to conduct experiments on Georgia's voting equipment *in its operational environment*. Opp. Ex. 182; Opp. Ex. 183; *see also* Opp. Ex. 255 ¶ 9.

265. During Mr. Lenberg's visit, the date on the Coffee County ICC was twice changed, both times on January 19, 2021, and never changed back, media was created to program a precinct scanner and a BMD, 559 ballots were scanned, and Misty Hampton gave him voting system data to take with him. Opp. Ex. 184

at 16-22, 117:1-10, 178:13-22, 178:1-2, 187:16-188:7, 251:15-20, 260-263, 263:5-265:5, 289:9-18; Opp. Ex. 185; Opp. Ex. 186; Opp. Ex. 187 at 11 n.17; Opp. Ex. 255 ¶¶ 9, 105-107; Opp. Ex. 255 Ex. 23 p. 1-2.

266. On January 17, 2021, an unknown entity uploaded Coffee County's November 2020 Cast Vote Records in json format to a public internet site, long before the json format Cast Vote Records were permitted to be released as public records by Georgia's Secretary of State. Opp. Ex. 188.

267. These November 2020 Cast Vote Records in json format can only be created with access to Georgia's EMS software and specific election database. Opp. Ex. 188.

268. In the late evening to early morning hours of February 25-26, 2021, Mike Lindell—a leading "election denier" associated with the Trump Campaign—mysteriously flew to Coffee County during the night after flying to DC and Mar-a-Lago that same day. Opp. Ex. 189; Opp. Ex. 149 at 261:10-265:14; Opp. Ex. 150 at 155:4-22.

269. Also on February 25, 2021, (i) Misty Hampton and her assistant resigned under pressure from the Coffee County Board of Elections, and (ii) Conan Hayes (another renown “election denier” associated with the Trump campaign) suddenly accessed data taken from the Coffee County voting equipment on the SS ShareFile site after weeks of inactivity. Opp. Ex. 150 at 155:4-12; Opp. Ex. 190; Opp. Ex. 191; Opp. Ex. 179 at -137 to -138.

270. The day before, February 24, Ms. Hampton was on Mr. Lindell’s website. Opp. Ex. 172 at 24.

271. Text messages produced by former-Coffee County Board member, Ed Voyles, show that Misty Hampton received a request on February 4, 2021 from Kurt Olsen, an attorney who represents Mr. Lindell, asking that she call him. Opp. Ex. 192 at 104-105; Opp. Ex. 266 at 145:3-148:15.

272. When questioned about the purpose of Mr. Lindell’s February 25, 2021 trip to Coffee County and communications with Mr. Lindell, Ms. Hampton pled the Fifth Amendment. Opp. Ex. 173 at 160:16-163:11.

273. Jil Ridlehoover also pled the Fifth Amendment in response to questions about her involvement in the Coffee County breach that occurred in January 2021, and stated that people being at the Coffee County elections office on January 7, 2021 raised red flags for her. Opp. Ex. 193 at 166:6-11.

274. On February 26, 2021, the day after both Coffee County elections workers were suddenly forced to resign and escorted out of the elections office—which was the same day Mr. Lindell flew to Coffee County during the night—Fortalice prepared an “Incident Response” protocol at the direction of the SOS Office noting that [REDACTED] [REDACTED].” (emphasis added). The evidence collection process “ [REDACTED] [REDACTED].” The software provided by Fortalice to the SOS Office “ [REDACTED] [REDACTED].” Opp. Ex. 194 at -660 (emphasis added).

275. Internal timestamps of February 3, 2021 indicate that Fortalice was drafting the February 26, 2021 Incident Response protocol just one week after an SOS investigator visited the Coffee County Elections Office at the same time Mr.

Lenberg was impermissibly inside the room where the EMS server was located and was performing various tests on the equipment in that room. Opp. Ex. 194 at - 661; Opp. Ex. 210 at 35-52.

276. The Coffee County Elections Office reportedly was closed from February 26, 2021—the day after Misty Hampton and Jil Ridlehoover resigned under pressure from the Coffee County Board of Elections and Mike Lindell flew in during the night—until April 2021, when James Barnes was hired to replace Misty Hampton. Opp. Ex. 67 at 85:23-86:14; Opp. Ex. 150 at 156:15-19.

277. The changes made to Georgia’s voting system via the Coffee County equipment *in its operation environment* during Mr. Logan and Mr. Lenberg’s January 2021 visits were “abnormal and reckless” because they could prevent the system from functioning properly or accurately recording votes, whether intentionally or inadvertently. Opp. Ex. 255 ¶ 158.

278. Because of this risk, when unauthorized individuals have accessed election hardware, other states have decommissioned it, quarantined it, and not used it in future elections. Opp. Ex. 255 ¶ 163.

279. State Defendants replaced only Coffee County's EMS server and ICC when the SOS Office learned in May 2021 about a potential compromise of the voting system there involving Doug Logan and his now-defunct Cyber Ninjas organization. Opp. Ex. 195; Opp. Ex. 149 at 130:19-23; 132:4-10, 400:20-401:11; *see also* Opp. Ex. 255 ¶ 165.

280. State Defendants refused to replace the remainder of the equipment for over 18 months, until September 26, 2022. Opp. Ex. 196; Opp. Ex. 195; Opp. Ex. 197; Opp. Ex. 149 at 159:18-160:15; *see also* Opp. Ex. 198 at 10:4-11:10 (stating that it seemed like it would be prudent for SOS Office to replace all the Coffee County equipment).

281. The Coffee County voting equipment accessed during the January 2021 breach was used in subsequent elections. Opp. Ex. 195; Opp. Ex. 197.

282. State Defendants have refused to replace the EMS server and ICC that were used with that potentially infected equipment for over 18 months, leaving voters still subject to that server and ICC in elections. Opp. Ex. 149 at 160:1-15; Opp. Ex. 200 (declining to replace the new EMS server and ICC).

283. State Defendants have provided no evidence that they ever actually analyzed any of the equipment they took from Coffee County in June 2021 and later September 2022 for malware, other compromises, or other alterations that could have affected how it operated in elections where it was used, nor were there any audits of those elections. Opp. Ex. 138 at 402:13-24; Opp. Ex. 149 at 152:10-14; *see also* Opp. Ex. 75 ¶ 6.d. State Defendants' consultant, Mr. Persinger testified that he did not conduct any such analyses and was not asked to do so. Opp. Ex. 201 ¶ 52. And Dominion reportedly failed to access its own equipment taken from Coffee County despite the ease with which the passwords on both could have been circumvented and the fact that at least the ICC password should have been known to the SOS Office given it was known to James Barnes in Coffee County when the SOS Office took it. Opp. Ex. 149 at 211:19-216:2.

284. During her deposition, Cathy Latham asserted the Fifth Amendment in response to key questions, including whether she was ever in the County Coffee elections office room containing the EMS server and ICC, Opp. Ex. 249 at 25:9-11, and whether she had discussed anything concerning the situation regarding the January 2021 Coffee County breach with Eric Chaney, *id.* at 29:20-22.

285. Ms. Latham provided false testimony under oath during her deposition, testifying that she went to the Coffee County elections office after 4:00 pm on January 7, 2021, for “just a few minutes,” and only “walked into the front part” and “didn’t go into the office.” Opp. Ex. 249 at 133:23-134:11; 136:19-22. In reality, Ms. Latham escorted multiple people into the elections office and remained there for much if not all of the day from 11:37AM until 6:19PM. Opp. Ex. 150 at 39:17-23; Opp. Ex. 175 at 126:3-13, 291:13-18; Opp. Ex. 250 at 6, 8-9; Opp. Ex. 176 at 79; Opp. Ex. 251 at 6-10. Ms. Latham also did in fact enter Ms. Hampton’s office, which leads to the EMS server room where the SS team breached and copied the voting equipment there. Opp. Ex. 176 at 38-39; Opp. Ex. 150 at 41:7-16; Opp. Ex. 175 at 127:13-19; 234:14-22; Opp. Ex. 251 at 11-13.

286. Eric Chaney also asserted the Fifth Amendment to various questions during his deposition, including whether he filmed a video of Misty Hampton that was posted to YouTube containing sensitive passwords for the Coffee County voting equipment, including the EMS server, Opp. Ex. 151 at 35:15-37:24, why the Coffee County video surveillance from January 2021 would have been destroyed, *id.* at 55:15-22, and whether he saw anyone in the Coffee County elections office

who was not supposed to be there when he reviewed the video surveillance having to do with Ms. Hampton's resignation, *id.* at 61:21-62:4; Opp. Exs. 268-269.

287. Eric Chaney falsely testified under oath that, to his knowledge, Doug Logan, Paul Maggio, and Scott Hall had never been in the Coffee County election office, despite spending much of January 7, 2021 in that office with the three of them. Opp. Ex. 151 at 60:4-25.

2. Election Data from Coffee County was Uploaded to the Internet and Accessed by Dozens of Unauthorized Individuals

288. Paul Maggio of SS emailed Sidney Powell on January 8, 2021, writing that "[REDACTED]"
[REDACTED] Opp. Ex. 175 at 302:2-9; Opp. Ex. 178.

289. SS uploaded all data collected from Georgia's voting system—which included sensitive Dominion election software from nearly every component of that system—to a cloud-based ShareFile site. Opp. Ex. 175 at 215:22-216:8.

290. SS provided login credentials to download the data taken from Coffee County to various individuals identified by Sidney Powell and others. Opp. Ex. 255 ¶ 9; Opp. Ex. 175 at 215:22-216:8.

291. Login credentials to the SS ShareFile site were shared with others, leaving no complete trail of who had the ability to—and did—login and access the sensitive data taken from Georgia’s voting system. Opp. Ex. 253 at 87:2-89:8.

292. Anyone with login information could access the Georgia voting system data on SS’s ShareFile site. Opp. Ex. 175 at 176:12-177:12.

293. Records produced by Mr. Maggio of SullivanStrickler’s ShareFile site’s user activity show that at least ten individuals from all over the country, and even outside of the country based on identified locations, uploaded and downloaded Georgia voting system data. Opp. Ex. 179; Opp. Ex. 255 ¶ 9.

294. Benjamin Cotton, a cybersecurity consultant who was retained by known “election deniers” and admitted he conducted a forensic analysis of the Georgia voting system data taken from Coffee County, was among the individuals

who downloaded and reviewed the data. Opp. Ex. 253 at 105:19-106:6; Opp. Ex. 256 at 2; Opp. Ex. 262.

295. The Georgia voting system data taken from Coffee County still existed on Mr. Cotton's home computer in Montana as of August 2022. Opp. Ex. 253 at 130:9-11 ("Q: Do you still have the Dominion data files from Coffee County? A: Yes.").

296. James Penrose provided his credentials to Mr. Cotton for Mr. Cotton to access the ShareFile account and download election software and data while logged in as Penrose. Opp. Ex. 253 at 87:2-89:8.

297. At least ten individuals across the country and even outside the U.S. based on the identified locations in the logs downloaded and uploaded sensitive Georgia voting system data. Opp. Ex. 179; Opp. Ex. 175 at 264:8-17; Opp. Ex. 255 ¶ 9.

298. Still other individuals had the Georgia voting system data taken from Coffee County shipped to them on hard drives. Opp. Ex. 258 at -100 (Jim

Penrose), at -098 (Stefanie Lambert at Michael Otra's apartment address); Opp. Ex. 184 at 204:3-13.

299. Doug Logan uploaded several zip files related to the Coffee County EMS server to the ShareFile site from a location in Florida on January 16, 2021. SS did not know why Logan uploaded these files, what they were, or where they came from. Opp. Ex. 179; Opp. Ex. 175 at 264:8-17.

300. Logan testified that he uploaded a forensic image he captured from the Georgia voting system while in the Coffee County elections office after having converted it into a virtual machine, which allows a viewer to "utilize it like it was the computer in order to take a look at the way the things operate, and more closely examine it like it was a local system you were using." Opp. Ex. 257 at 125:5-126:5.

301. Greg Freemyer, a SullivanStrickler employee who was involved in the firm's copying of Dominion election data from a county in Michigan, uploaded zip files to the ShareFile site from a location in New Jersey on January 24, 2021. Opp. Ex. 175 at 264:8-17; Opp. Ex. 300.

302. Scott Hall forwarded Alex Cruce the Coffee County ICC log and SLOG he received from Ms. Hampton over e-mail. Opp Ex. 265 at 51:5-22; 53:22-54:5; 85:8-17.

303. From Mr. Cruce's understanding, "election officials around the state of Georgia had been handing over SLOG files. It was a lot that actually were giving them to people." Opp Ex. 265 at 135:15-20³.

304. Kevin Skoglund found Cast Vote Records ("CVRs") (data which show how a tabulator interpreted each ballot) from the November 2020 General Election in Coffee County publicly available on the Internet with an upload date of January 17, 2021. Opp. Ex. 301 ¶ 2-5, 17-22.

305. In Coffee County, a few rogue elections officials were able to provide access to sensitive Georgia voting system equipment and software used in elections in Coffee County and the other 158 counties in Georgia, which all use the same

³ The David Cross (of Georgia) mentioned in this excerpt works in money management and met Mr. Cruce when "[Mr. Cruce] rolled [his] IRA into an account with him." Opp Ex. 265 at 54:9-55:2. He is *not* the David D. Cross who represents Curling Plaintiffs in this litigation.

Dominion election software and the same types of Dominion election equipment.

Opp. Ex. 149 at 144:24-145:11; 147:10-15.

306. The access that Paul Maggio, Karuna Naik, Jennifer Jackson, and Jim Nelson (“the SS Team”), Scott Hall, Doug Logan, and Jeffrey Lenberg obtained in January 2021 to the Dominion voting equipment used in Coffee County, Georgia, in or around January 2021 was not authorized under Georgia law. Opp. Ex. 195.

307. The access Scott Hall, Doug Logan, Jeffrey Lenberg, the SS Team, Ben Cotton, Alex Cruce, and the numerous other individuals had to download proprietary Dominion software and Georgia election data from Georgia voting system equipment in Coffee County in or around January 2021 was not authorized under Georgia law. Opp. Ex. 195; Opp. Ex. 262.

308. The dissemination by the SS Team of Dominion software and voting data that was copied from the Georgia voting system equipment used in Coffee County, Georgia, in or around January 2021 was not authorized under Georgia law. Opp. Ex. 195.

309. The changes Doug Logan, Jeffrey Lenberg, and the SS Team made in January 2021 to one or more components of the Georgia voting system equipment used in Coffee County, Georgia, were not authorized under Georgia law. Opp. Ex. 195.

310. In January 2021, the Coffee County Election Supervisor did not have the legal authority to provide Scott Hall, Doug Logan, Jeffrey Lenberg, or the SS Team access to the Georgia voting system equipment used in Coffee County, Georgia. Opp. Ex. 195.

311. In January 2021, the Coffee County Election Supervisor did not have the legal authority to allow Scott Hall, Alex Cruce, Doug Logan, Jeffrey Lenberg, or the SS Team to copy Dominion software or voting data from the Georgia voting system equipment used in Coffee County, Georgia. Opp. Ex. 195.

312. In January 2021, the Coffee County Election Board, including individual members, did not have the legal authority to provide Scott Hall, Doug Logan, Jeffrey Lenberg, or the SS Team access to the Georgia voting system equipment used in Coffee County, Georgia. Opp. Ex. 195.

313. In January 2021, the Coffee County Election Board, including individual members, did not have the legal authority to allow Scott Hall, Doug Logan, Jeffrey Lenberg, or the SS Team to copy Dominion software or Georgia voting data from the Georgia voting system equipment used in Coffee County, Georgia. Opp. Ex. 195.

3. The Coffee County Breach Poses a Serious Threat to the Security of Future Georgia Elections

314. Dr. Halderman and Kevin Skoglund examined a series of forensic images from Coffee County's EMS server and other components of the Georgia's voting system and found that the "risk that a future Georgia election will be attacked materially increased with the outside group(s)'s copying and distribution of the proprietary software that operates Georgia's election system and specific system configurations." SullivanStrickler hard drive produced on Aug. 12, 2022; Opp. Ex. 75 ¶ 6; *see also* Opp. Ex. 255 ¶ 9(i); Opp. Ex. 149 at 52:21-53:6; Opp. Ex. 31 at 192:16-193:6.

315. Adversaries, including one or more of those involved with the January 2021 Coffee County breach, may use the software taken in that breach in disinformation campaigns or study it to learn how to subvert its operation through

malware, reprogramming, or disabling defenses. Opp. Ex. 255 ¶ 9(i); Opp. Ex. 257 at 125:5-126:5; Opp. Ex. 253 at 105:19-106:6.

316. The January 2021 Coffee County breach and others like it portend easier access to equipment to put manipulations into effect—in Coffee County strangers and outsiders were given free rein to key components of Georgia’s voting system *in its operational environment* for hours and days. Opp. Ex. 255 at ¶ 9(i).

317. The implications of the January 2021 Coffee County breach require that the recommendations of election security experts, as well as CISA, should be implemented fully and urgently throughout Georgia. Opp. Ex. 255 at ¶ 9(i).

318. The January 2021 Coffee County breach was by any measure a consequential breach of Georgia’s voting system security—in its operational environment no less. Opp. Ex. 255 ¶ 9(h).

319. Georgia’s access controls to protect election hardware and software are obviously insufficient in light of the January 2021 Coffee County breach. Opp. Ex. 255 ¶ 9(h).

320. The data collected in the January 2021 Coffee County breach includes sensitive, access-restricted software from almost every component of Georgia's current voting system. Opp. Ex. 255 ¶ 9(h); Opp. Ex. 175 at 144:12-147:5, 290:7-14, 302:2-9; Opp. Ex. 75 ¶ 12.

321. Control over sensitive voting equipment software and data cannot be reestablished after its distribution like occurred with the in the January 2021 Coffee County breach, and all of Georgia's counties and other states using the same or similar Dominion software or equipment must now endure the increased risk attendant to that breach as a result. Opp. Ex. 255 ¶ 9(h); Opp. Ex. 75 ¶¶ 6, 40; Opp. Ex. 149 at 52:21-53:6; Opp. Ex. 138 at 192:16-193:6.

322. All users of the Coffee County EMS server share a single account, rather than assigning users accounts with differing levels of access based on role and need. This single account has administrator privileges, such that any authorized user could bypass security controls and alter software, election data, and log files. Opp. Ex. 75 ¶¶ 45, 47-48.

323. The hard drive on the Coffee County EMS server and ICC workstation reportedly taken by the SOS Office in June 2021 are both unencrypted,

even though the operating system supports the full-disk encryption that is standard for most modern smartphones and corporate laptops. Such unencrypted systems allow anyone with physical access to use widely available methods to bypass a Windows login password and gain access. Opp. Ex. 175 at 172-174; *see also* Opp. Ex. 75 ¶ 43.

324. Both the Coffee County EMS server and ICC reportedly taken by the SOS Office in June 2021 operate on outdated software lacking critical security updates. The EMS server uses an August 2016 version of Windows, and Georgia has never installed any system security patches. Opp. Ex. 75 ¶ 29.

325. Windows has released some 380 software updates for the version of Windows used on the Coffee County EMS server reportedly taken by the SOS Office in June 2021, including 165 “critical” updates that fix vulnerabilities that hackers are already actively exploiting. Opp. Ex. 75 ¶ 31.

326. The Coffee County ICC workstation reportedly taken by the SOS Office in June 2021 uses a July 2015 version of Windows installed on the workstation in November 2019. Since then, the State has not installed any security updates on the ICC workstation. Opp. Ex. 75 ¶¶ 30, 27.

327. Windows has released 184 software updates for the version of Windows used on the Coffee County ICC workstation reportedly taken by the SOS Office in June 2021, of which 101 are critical. Opp. Ex. 75 ¶ 30.

328. The web browser history file contained in the forensic image of the ICC reportedly taken by the SOS Office in June 2021 indicates the system was at least briefly connected to the Internet on November 25, 2019, the same day Windows was installed. Opp. Ex. 75 ¶ 25.

329. State Defendants tout their use of hash testing as ensuring the integrity of the software used in the Georgia's voting system. *See e.g.*, Opp. Ex. 48 at 36:7-11, 38:9-17.

330. But the forensic images of the Coffee County EMS server reportedly taken by the SOS Office in June 2021 showed that the hash testing tool used during acceptance testing verified the hash values of only four files on the EMS server, out of 700 Dominion software application files and 27,000 files containing executable on the system. Thus, although there are numerous files on the system that could be modified by malware, Georgia or its vendor inspected only a tiny fraction during hash testing. Opp. Ex. 75 ¶ 40.

331. The dissemination of the Dominion software taken from the Georgia voting system equipment used in Coffee County and all other Georgia counties by SS and others provides countless individuals and entities a “roadmap” to hack Georgia elections—and the January 2021 Coffee County breach confirms that access to the system is not hard to procure. Opp. Ex. 75 ¶ 6; Opp. Ex. 149 at 52:21-53:6; Opp. Ex. 138 at 192:16-193:6.

332. The KNOWink Poll Pads used in Coffee County were used to stream Netflix content over the internet. Opp. Ex. 172 at 19; Opp. Ex. 173 at 49:22-50:11; Opp. Ex. 151 at 120:2-121:6.

333. The Coffee County EMS computer and ICC tabulation computer had Windows game applications installed. Opp. Ex. 172 at 20; Opp. Ex. 173 at 50:15-52:9; Opp. Ex. 151 at 121:7-122:6.

L. State Defendants Ignored All Indications of the Coffee County Breach, until Plaintiffs began to Uncover the Facts.

334. State Defendants claim the SOS Office opened an investigation into the January 2021 Coffee County breach as soon as the SOS Office learned of an

allegation made by Scott Hall that the equipment had been infiltrated in February 2022. Opp. Ex. 272 at 21:20-23; Opp. Ex. 149 at 274:5-277:18.

335. The SOS Office wrongly asserted that, when it purportedly opened an investigation in March 2022, “the call from Mr. Hall was the sole basis for this concern that there was some sort of compromise of the system[.]” Opp. Ex. 272 at 39:5-8.

336. In December 2020, the SOS opened an investigation into a YouTube video showing Coffee County Election Supervisor Misty Hampton demonstrating ways to manipulate Georgia’s voting software, with the EMS server password visible on her computer monitor. Opp. Ex. 286 at 2-3; Opp. Ex. 76.

337. The SOS sent an investigator to Coffee County who visited the elections office at least three times: on December 11, 2020 and January 20 and 26, 2021. Opp. Ex. 209 at 1-3, 18-25, 35-52.

338. During the investigator’s third visit on January 26, 2021, Jeffrey Lenberg was present in the Coffee County elections office at the same time as the

investigator, working in Misty Hampton's office or in the EMS server room which is accessed from her office. Opp. Ex. 210 at 35-52.

339. The investigator did not appear to question Mr. Lenberg's presence or pursue the issue of unauthorized personnel being allowed in sensitive areas of the Coffee County elections office during his January 2021 visits. Opp. Ex. 210 at 35-52.

340. On September 28, 2021, the investigator submitted his summary of findings related to his Coffee County investigation. Opp. Ex. 76.

341. The summary found that the Coffee County Board of Elections and Misty Hampton violated SEB RULE 183.1-12-.05(3) Security of Voting System Components at County Elections Office or Designated County Storage Area (for leaving a critical door unlocked). Opp. Ex. 76 at 5.

342. The summary makes no mention of any unauthorized personnel in the Coffee County elections office. Opp. Ex. 76 at 5.

343. The SOS Office did not act on the finding that Misty Hampton violated state regulations insofar as she received no repercussions from the SOS Office or another Georgia agency for those violations. Opp. Ex. 76 at 5.

344. Robert Sinners was a key “election denier” on the ground in Georgia actively supporting Trump’s “Big Lie” about the November 2020 election. Opp. Ex. 211 at 122:12-16, 244:7-9.

345. Mr. Sinners initially claimed under oath *not* to have organized a lawsuit filed against Coffee County by Shawn Still in or around December 2020/January 2021, but then admitted to flying to Coffee County on December 12, 2020, with Alex Kaufman in a private plan to serve as a notary for declarations collected from declarants he and Kaufman recruited at a local Coffee County steakhouse; he further admitted that he and Kaufman typed up the declarations, printed them out at a local hotel, and got them signed by the declarants and notarized by Mr. Sinners during their 12 to 18-hour stay in Coffee County. Opp. Ex. 211 at 35:11-42:5.

346. Mr. Sinners testified that he did not know why the Shawn Still lawsuit was dropped on January 7, 2021, the same day that the breach of Georgia’s voting

system occurred in the Coffee County Election Office involving the SS Team among others. Opp. Ex. 211 at 42:6-10, 122:12-16, 244:7-9.

347. Mr. Sinners claimed to have had limited interaction with Eric Chaney and Misty Hampton because Coffee County was a “low-priority county,” and concerns about the voting system were not within the scope of his role. Opp. Ex. 211 at 32:14-34:15.

348. Mr. Sinners was in touch with Eric Chaney and Misty Hampton around the same time regarding the November 2020 election, including ask for and receiving a letter to Secretary Raffensperger about Coffee County’s inability to certify the election. Opp. Ex. 211 at 72:17-19, 82:13-86:17.

349. On the evening of January 7, 2021, just as SS completed its work in the Coffee County elections office, Mr. Chaney sent Ms. Hampton Mr. Sinners’ personal cellphone number and told her to switch to Signal (which enables users to delete encrypted messages they send and receive from all other user’s devices in the same conversation, unlike other messaging apps that enable a user to delete messages only from their own device). Opp. Ex. 211 at 110:19-111:13; Opp. Ex. 172 at 23.

350. The SOS Office hired Mr. Sinners in February 2021, shortly after Mr. Lenberg spent five days accessing and testing sensitive components of Georgia's voting system in its operational environment in Coffee County; and the SOS Office has since promoted Mr. Sinners to a senior communications role. Opp. Ex. 211 at 123:20-124:15.



351. In November 2020, individuals at the Robbins and Taylor English law firms appear to have assisted a movement in Georgia at that time looking to raise doubts about the results of the 2020 Presidential election, including by connecting the team with Robert Sinners, who also was part of that same movement. Opp. Ex. 212 at 2-8.

352. On May 6, 2021, Dominion circulated to Georgia counties a customer notification "[REDACTED]
[REDACTED]." Opp. Ex. 213.

353. Also on May 6, 2021, Ms. Hampton's successor as Coffee County Elections Supervisor, James Barnes, emailed Georgia's then-State Elections Director Chris Harvey to report that he found a Cyber Ninjas business card for Doug Logan at the base of Hampton's former computer, and that this was alarming

to him, because it suggested that “[i]f [Misty] did not use them, she was at the very least in contact.” Opp. Ex. 127.

354. Mr. Harvey directed the SOS Office’s chief investigator, Frances Watson, to investigate whether there had been contact between Doug Logan and anyone at the Coffee County Elections Office. Opp. Ex. 127.

355. The SOS Office’s investigator spoke with James Barnes who said that “
.” Opp. Ex. 214; Opp. Ex. 215; Opp. Ex. 149 at 77:23-81:2.

356. In a recorded interview, Secretary Raffensperger later claimed that his office conducted a thorough investigation of the Coffee County incident in May 2021, including interviewing Misty Hampton Opp. Ex. 216.

357. No one had interviewed Ms. Hampton on behalf of the SOS Office or State of Georgia for well over a year after she resigned her position in the Coffee County Elections Office. Opp. Ex. 173 at 237:19-22.

358. Around the time that James Barnes reported the Cyber Ninja business card to the SOS Office, he also reportedly realized that the password to Coffee County’s EMS server—a password provided by the SOS Office—no longer worked. Opp. Ex. 67 at 108:3-109:4.

359. James Barnes reported the issue to SOS’s Center for Elections, which promptly replaced the EMS server and the computer attached to the ICC on or about June 8, 2021. Opp. Ex. 67 at 108:3-109:4.

360. Mr. Barnes understood the SOS Office replaced the Coffee County EMS server and ICC workstation in or around June 2021 for fear that it was compromised, per the Cyber Ninjas card. Opp. Ex. 67 at 159:25- 162:12.

361. James Persinger identifies himself as a “computer forensic and cybercrime expert” retained by State Defendants’ counsel in or about *May 2021*—the same time James Barnes alerted the SOS Office to the Cyber Ninjas card in the Coffee County Elections Office and Chris Harvey directed the SOS Office Investigative Unit to investigate potential unauthorized access to the voting equipment in Coffee County. Opp. Ex. 201 ¶¶ 3, 11.

362. On or about June 29th, 2022 State Defendants’ counsel requested that Persinger take possession of the Coffee County EMS server and Coffee County Workstation computer to determine if he could gain access to the EMS server, discover when the EMS server was last access and who had accessed it, determine if the EMS server was connected to the Internet after the password was changed, determine whether the EMS server had been forensically imaged before he took possession of it, or determine if any other devices had been connected to the EMS server that were inconsistent with normal operations—but remarkably, State Defendants’ counsel reportedly did not inform Persinger that it was potentially evidence related to an ongoing lawsuit and did not direct him to take reasonable measures to preserve the server’s data. Opp. Ex. 201 ¶¶ 12, 14.

363. Sometime around or shortly after June 29, 2022, Michael Barnes, the Director of the Center for Elections Systems at the SOS’s Office, asked Persinger to reset the EMS server password to a known password. Opp. Ex. 201 ¶ 15.

364. Persinger took possession of the Coffee County EMS server on or around July 1, 2022. At that time, he and Michael Barnes executed an *evidence* chain of custody form to document the change in possession of the EMS server and

workstation, even though Persinger claims under oath nobody informed him that it was potentially evidence related to an ongoing lawsuit. Opp. Ex. 201 ¶¶ 16, 17.

365. Persinger began his work on the Coffee County EMS server on or about July 5, 2022. He started by creating a forensic image of the EMS server. Opp. Ex. 201 ¶ 22.

366. Upon examination, Mr. Persinger noted that the internal clock on the Coffee County EMS server was incorrect. Opp. Ex. 201 ¶ 20.

367. Persinger reset the Coffee County EMS server password after he created a forensic image of the server—on or about July 5, 2022. Opp. Ex. 201 ¶ 23.

368. Persinger claims he did not alter any other files on the Coffee County EMS server other than one file, associated with the password reset. Opp. Ex. 201 ¶ 49.

369. Dr. Halderman compared the forensic image of the Coffee County EMS server made by Persinger on or about July 5, 2022 to other forensic images of

that same EMS server, including created by the SS Team in January 2021 and another created on or about September 22, 2022, by Plaintiffs' litigation consultant. Opp. Ex. 187 ¶¶ 11-12, 15.

370. If Persinger had only changed one file associated with his password reset on the Coffee County EMS server, the July 5, 2022 and September 22, 2022 forensic images would be identical except for that single file. Opp. Ex. 187 ¶ 12

371. Persinger in reality caused *hundreds* of changes to the Coffee County EMS server. Opp. Ex. 187 ¶¶ 10, 16. While the server was in Mr. Persinger's possession, 185 new files or folders were created, 349 were deleted, 21 were appended to, and 719 were otherwise modified. Opp. Ex. 187 ¶ 16, Ex. A.

372. The files that Persinger altered include files that contain evidence of what occurred during the January 2021 Coffee County breach. Opp. Ex. 187 ¶ 18. These include election project databases, Windows registry files (which store the system configuration and user settings), and numerous kinds of log files. Opp. Ex. 187 ¶ 18. Log files are files that document important activities relating the EMS server's operation. Opp. Ex. 187 ¶ 19. They are a primary source of information for experts when analyzing a computer's prior activity. Opp. Ex. 187 ¶ 19.

373. Persinger’s changes to the Coffee County EMS server are not standard forensic practice. Opp. Ex. 187 ¶ 4. Standard practice would be to perform all analysis using a *copy* of the data from the server, not to perform analysis on the original server itself. Opp. Ex. 187 ¶ 4.

374. Apart from a single generic acceptance testing document for an EMS server, Defendants claim they have no documents—including emails, text messages, chain of custody forms, etc.—regarding this unusual replacement of a county’s EMS server and ICC workstation (which State Defendants represented to this Court in September 2022 was a significant undertaking and that is why they declined to replace that same equipment in Coffee County at that time when replacing other voting system components then). Opp. Ex. 197; *see also* Opp. Ex. 67 at 118-21, 131-32, 134-36 (testifying that no documentation of the events exists); Opp Ex. 202 (noting that State Defendants had not preserved additional documents to produce, despite having had knowledge that the server was potentially compromised and so would be highly relevant to Plaintiffs’ case).

375. State Defendants made no serious investigative efforts to look into the January 2021 Coffee County breach until after Plaintiffs began investigating it in the spring of 2022. State Defendants did not refer the matter to the GBI until

August 2022. Opp. Ex. 150 at 176:25-177:22; Opp. Ex. 151 at 167:4-18; Opp. Ex. 203.

376. However, from March 14, 2022 to present, State Defendants repeatedly claimed an “ongoing investigation” was underway regarding the January 2021 Coffee County breach in order to shield discovery regarding that breach. Opp. Ex. 204 at 5; Opp. Ex. 203; Opp. Ex. 205; Opp. Ex. 206; Opp. Ex. 207; Opp. Ex. 208.

377. State Defendants previously asserted that the state investigation of the January 2021 Coffee County breach would be completed and Georgia would be able resolve any security issues before the November 2022 elections—but that did not happen. Opp. Ex. 142 at 53:11-17, 80:3-5.

378. Gabriel Sterling, the SOS Office’s COO, publicly announced in April 2022 that there was no evidence of a voting system breach in Coffee County, claiming that “it didn’t happen”—which was not an accurate statement. Opp. Ex. 217.

379. On October 1, 2022, Gabriel Sterling re-tweeted a statement by Dr. Ben Adida, State Defendants’ prior expert in this case and a SOS Office election consultant, that there was no cause for concern about the January 2021 Coffee County breach because it lasted only a few hours, even though the statement was inaccurate. Opp. Ex. 149 at 46:9-48:5; Opp. Ex. 86.

380. Sixteen months after Mr. James Barnes reported the Cyber Ninjas business card and the purported EMS server password issue to the SOS Office—and just three months before the November 2022 midterm elections—State Defendants suddenly acknowledged that they had “questions” about the January 2021 Coffee County breach and referred the issue to the Georgia Bureau of Investigations. *See* Opp. Ex. 142 at 11:7-17.

381. On August 15, 2022, an investigation was opened by the GBI relating to the “Coffee County Server Security”—no status report or information has been provided about that investigation in months, and nobody has received any criminal charges regarding the January 2021 Coffee County breach. Opp. Ex. 149 at 115:4-24; Opp. Ex. 218.

M. Georgia’s Election System Also Lacks Procedural Safeguards Because it is Un-Auditable.

382. Under Georgia law, an RLA is a protocol using “statistical methods” that is “designed to limit to acceptable levels the risk of certifying a preliminary election outcome that constitutes an incorrect outcome.” O.C.G.A. 21-2-498(a)(3).

383. A risk-limiting audit (“RLA”) is not a tabulation; rather, an RLA statistically checks whether an accurate manual count of the paper trail would find the same winner(s). Opp. Ex. 219 ¶ 14.

384. Georgia has never conducted a legitimate RLA. Opp. Ex. 220 at 48:3-4; Opp. Ex. 221 ¶¶ 23-32; SMF Ex. 44 ¶¶ 13-17; SMF Ex. 42, Mar. 2022 Stark Decl. at 31 ¶ 87(g).

385. In a proper RLA, more and more reliable, voter-verified ballots are examined until either (a) the voter-verified selections listed on the examined ballots give convincing evidence that the reported winners really won or (b) the voter-verified selections listed on all the ballots have been manually inspected so the correct outcome is known. Opp. Ex. 219 ¶ 26.

386. In Georgia, the initial QR code tabulation is the *only* tabulation in an election, unless there is a full, hand recount. Opp. Ex. 84 at Ex. B, Dominion Solution Order, § 3.1; Opp. Ex. 71 at 72:2-9; Opp. Ex. 85 at 71:3-72:8.

387. The audit and hand count of the 2020 Presidential race in Georgia did not check the outcome of the election, and the thing it was positioned to check—the tabulation of validly cast ballots—was not checked properly. SMF Ex. 42 ¶¶ 23-45.

388. The hand recount conducted for the 2020 Presidential election relied upon a tool that Mr. Richard Barron, former Fulton County Election Supervisor, called “a complete joke” – a piece of software called “Arlo” that was “not built” for the purpose of an audit. Opp. Ex. 70 at 147:7-149:14; Opp. Ex. 48 at 202:10-203:24.

389. Georgia’s November 2022 Presidential election audit “was not a genuine RLA, nor an effective audit.” SMF Ex. 44 at 4.

390. Georgia law only requires an RLA of a single statewide race every two years. Ga. Comp. R. & Regs. 183-1-15-.04.

391. The SOS Office called such infrequent auditing as required by Georgia law “crazy.” Opp. Ex. 149 at 325:3-25.

392. Philip Stark, a leading expert in election auditing, has testified that “[a] risk-limiting audit of one contest every two years is not enough, no matter how rigorous that audit is.” Opp. Ex. 222 ¶ 17.

393. Post-election audits will only flag an incorrect election outcome if they are based on a trustworthy paper trail (i.e., voter-*verified* selections that are tabulated on a paper ballot) produced by a voting system that is software independent (i.e., immune to software changes altering an election outcome without detection). SMF Ex. 55 at PDF p. 3, ¶ 4; Opp. Ex. 90 ¶ 8; SMF 44 ¶ 18.

394. If there is no trustworthy paper trail, a true tabulation audit is not possible, because even an accurate full manual recount would not necessarily reveal who won. SMF Ex. 55 at PDF p. 3, ¶ 4; Opp. Ex. 92 at 1-2; SMF Ex. 42 ¶ 85; Opp. Ex. 56 at 30:17-31:2.

395. Unlike HMPBs, BMD ballots do not produce a trustworthy paper trail, even if proper custody procedures are followed. This is because a malfunctioning

or compromised BMD could print a human-readable text summary that does not match what the voter selected on the touchscreen or what the QR encoded. Opp. Ex. 90 ¶¶ 5, 10 n.31, 19 n.11; SMF Ex. 44 ¶ 9; Opp. Ex. 220 at 19:9-20:06, 20:23-21:14; Opp. Ex. 55 at 95:23-96:6; see also Opp. Ex. 128 at 72:2-15; Opp. Ex. 129 at 67:21-69:19; 100:17-101:13; Opp. Ex. 141 at 35:17-36:9; Opp. Ex. 130 at 34:1-37:2; Opp. Ex. 99 at PDF p. 165, ¶¶ 6, 15; Opp. Ex. 56 at 35:15-24; 37:16-38:7, 48:1-9; Opp. Ex. 87 at 43:11-14, 44:6-8, 45:17-46:1, 46:4-11, 81:24-82:2, 123:21-124:8; Opp. Ex. 105 at 285:4-14, 301:2-24; *see also* Opp. Ex. 48 at 81:15-84:1; Opp. Ex. 219 ¶ 32; Opp. Ex. 54 ¶¶ 41, 55; SMF Ex. 44 ¶ 5; Opp. Ex. 223 ¶¶ 11, 13, 21; Opp. Ex. 224 ¶ 6(c); SMF Ex. 42 ¶ 86; Dkt. 1131, Halderman Report at 6-7; Dkt. 1589, Feb. 2, 2023 Stark Decl., ¶ 2, Ex. 1.

396. Election security experts recognize that audits of elections conducted primarily on BMDs cannot reliably detect whether computer errors or hacking altered votes or election results. Opp. Ex. 99 at PDF p. 165, ¶¶ 6, 15; SMF Ex. 44 ¶ 5; Dkt. 1589, Feb. 2, 2023 Stark Decl., ¶ 3, Ex. 2; Opp. Ex. 55 at 95:23-96:6; Opp. Ex. 92; Opp. Ex. 56 at 48:5-9, 109:1-3, 135:23-136:2; *see also* Opp. Ex. 91 at 77 (“[T]here is no audit remedy that can confirm the reliability and accuracy of the BMD system, as Dr. Stark has stressed.”).

397. Even if Georgia conducted a post-election audit for every election contest—and even if those all properly-conducted RLAs—that would not mitigate the security risks of Georgia’s election system, because audits cannot confirm that any votes were accurately recorded. *See, e.g.*, SMF Ex. 42 ¶ 87(b); SMF Ex. 55 at PDF p. 3, ¶ 10; Opp. Ex. 90 ¶ 10.); Opp. Ex. 71 at 70:9-12, 173:8-13.

398. Even if elections conducted primarily on BMDs could be properly audited by RLAs, Georgia would need to change its election procedures—including the physical security of the voted ballots, the physical accounting for ballots, and checks of chain of custody—to conduct a proper one. Opp. Ex. 220 at 19:9-20:06, 20:23-21:14; SMF Ex. 44 ¶ 6).

399. To conduct what qualifies as an RLA, Georgia would also need the ability to correct an election outcome before certification if the outcome is wrong. Opp. Ex. 220 at 48:11-12.

400. Current Georgia law does not require a full manual recount to correct inaccurate results. *See* Opp. Ex. 225 ¶¶ 27-28; Opp. Ex. 220 at 48:9-25; Opp. Ex. 93 ¶ 15.

401. If there are significant security vulnerabilities left unremedied in an election system like Georgia’s, “the effects of stealing individual voters’ votes and even altering election outcomes are likely to go undetected. . . .” Opp. Ex. 93 ¶ 15; *see also* Opp. Ex. 287.

402. Optical scanner hacking, contrary to BMD hacking, is “reliably detectable [through RLAs] and . . . is fully correctable without an election do-over,” particularly because such hacking does not affect the paper ballot itself, which then can serve as an independent, reliable record of the voter’s selections if the ballot contains voter-verified selections that are used for tabulation. Opp. Ex. 56 at 132:24-133:12; *see also* SMF Ex. 59 ¶ 75.

403. Hand-marked paper ballots allow officials to conduct a secure and accurate election even in the presence of voting equipment that may have been hacked. Opp. Ex. 56 at 76:20-77:5.

N. Curling Plaintiffs are Georgia Electors Who Have Suffered Particularized Harm.

404. Georgia’s current voting system has forced Donna Curling to choose between (1) voting on a system she does not believe will reliably count her vote

using a ballot she cannot verify and which does not leave a software-independent paper trail; and (2) voting absentee using a paper ballot. Opp. Ex. 226 ¶ 5.

405. Because Ms. Curling was concerned that Georgia's in-person DRE system could not securely record her votes for the June 2017 election, she elected to vote using an absentee ballot. Opp. Ex. 273 ¶ 12.

406. Before the June 2017 election, Ms. Curling called the election office to determine the procedures for voting absentee and was told she could receive an absentee paper ballot by going to the County Annex and filing a request. When Ms. Curling went to the County Annex on the Friday before Election Day to receive an absentee ballot, she was informed that she could only receive an absentee ballot by mail. Opp. Ex. 273 ¶ 7-11.

407. Ms. Curling requested an absentee ballot for the June 2017 election and it arrived on June 19, 2017, the day before Election Day. Opp. Ex. 273 ¶ 7-11.

408. When Ms. Curling took her absentee ballot for the June 2017 election to her precinct, she was informed that she must instead take it to the county election office. Opp. Ex. 273 ¶¶ 7-11.

409. Ms. Curling took her absentee ballot for the June 2017 election to the county election office and confirmed with the office clerk that she had followed the proper procedures. Opp. Ex. 273 ¶¶ 2-5, 7-11.

410. Ms. Curling did not learn until filings in this case that her June 2017 ballot was not counted and she had been disenfranchised. Opp. Ex. 273 at 4; SMF Ex. 17, Dkt. 627 ¶ 15.

411. Following Ms. Curling's discovery that her absentee ballot in the June 20, 2017 election was not counted, she reluctantly voted on DRE machines in subsequent elections. Opp. Ex. 273 ¶ 12.

412. Ms. Curling also lacks confidence in Georgia's BMD system because it is susceptible to manipulation and not transparent, and voters using Georgia's BMDs cannot verify their ballots since the barcode—not the human-readable portion of the paper ballot—is used to tabulate votes. Opp. Ex. 228 at 67:7-17, 73:15-23, 83:15, 95:25-96:10, 99:16-23, 102:6-12.

413. Ms. Curling did not receive an absentee ballot for the August 2020 election, even though she timely submitted an application for one. Dkt. 1598, Feb. 10, 2023 Curling Decl. ¶ 10.

414. Ms. Curling reluctantly again attempted to vote absentee in the 2020 Presidential primary, because of her concerns about verifying her vote with Georgia's BMD system. Opp. Ex. 227 ¶¶ 6, 12; Opp. Ex. 228 at 75:3-6.

415. Although she applied for an absentee ballot six weeks before the 2020 Presidential primary election, Ms. Curling did not receive her ballot until the day before election day. Opp. Ex. 227 ¶ 6; Opp. Ex. 228 at 112:15-24.

416. Because her absentee ballot for the 2020 Presidential primary election arrived one day before election day, Ms. Curling took her ballot to a drop box, rather than mailing it in, and did not learn until filings in this case that her ballot was not counted and she had been disenfranchised. Opp. Ex. 227 ¶ 4; SMF Ex. 17, Dkt. 627 ¶ 15.

417. When Ms. Curling voted in person on Georgia’s BMD system in a municipal election, she “ha[d] no way of knowing” if her vote counted. Opp. Ex. 228 at 41:7-12, 42:24-43:4, 83:16-19, 99:22-23.

418. Ms. Curling intends to vote absentee in the future despite its burdens and challenges, including the possibility of disenfranchisement, because she cannot trust Georgia’s BMD system. Opp. Ex. 228 at 74:14-19; 112:2-113:2; 124:18-125:5; Opp. Ex. 226 ¶ 12; Opp. Ex. 227 ¶¶ 7, 11.

419. If Georgia implemented a voting system that provides voters with hand-marked paper ballots, such that she could review and verify her votes, Ms. Curling would find it less risky to cast an in-person ballot and she would exercise her right to vote in-person on Election Day. Opp. Ex. 227 ¶ 8.

420. Secretary Raffensperger has agreed that Fulton County Defendants’ actions have disenfranchised voters like Ms. Curling. Opp. Ex. 229 (“The Department of Justice needs to take a long look at what Fulton County is doing and how their leadership disenfranchises Fulton voters through incompetence and malfeasance.”).

421. Ms. Price had been concerned about DRE machines since the early 2000s and filed a complaint about the DRE machines in 2006. Opp. Ex. 230 at 77:9-78:24.

422. Plaintiff Donna Price voted in person until about 2018, at which point she started voting absentee after hearing what had happened in Kennesaw. Opp. Ex. 230 at 77:9-16.

423. Under Georgia's current BMD system, Ms. Price is forced to choose between voting with a ballot that she cannot verify or voting absentee. Opp. Ex. 230 at 45:7-46:12

424. Voting absentee has its own barriers for Ms. Price; for example, Ms. Price cannot see that the ballot goes into a lockbox or scanner like her fellow voters who vote in person can. Opp. Ex. 230 at 45:7-46:12; Opp. Ex. 231 ¶¶ 8, 11; Opp. Ex. 234 ¶¶ 7-8.

425. If she were to vote on a Georgia BMD, Ms. Price would not be able to verify the selections she made because she cannot read QR code, thus, Ms. Price

would have no primary record of the selections she made. Opp. Ex. 230 46:13-47:14; Opp. Ex. 234 ¶¶ 8-10.

426. Without a durable, software-independent, voter-verified record to audit, Ms. Price has no confidence that the results of a given election conducted using Georgia's BMD system will be accurate and reliable. Opp. Ex. 234 ¶ 8.

427. If she were to vote on a Georgia BMD, Ms. Price believes she would merely be going through the motions of an action that simulates voting, while giving up her vote to whatever determines what is in the QR code. Opp. Ex. 230 at 48:1-15.

428. Ms. Price is concerned that Georgia does not perform risk-limiting audits that could help secure her right to vote with an otherwise reliable voting system. Opp. Ex. 230 at 45:7-46:12.

429. Because of Georgia's BMDs' infirmities, Ms. Price plans on voting on an absentee paper ballot in future elections even though she finds that absentee voting imposes other burdens. Opp. Ex. 231 ¶ 8.

430. On January 27, 2020, Ms. Price requested an absentee ballot for the March 24, 2020 election, which she received on February 21, 2020. Opp. Ex. 231 ¶ 12.

431. Ms. Price promptly mailed her completed absentee ballot back ahead of the primary, which was then scheduled for March 24, 2020. Opp. Ex. 231 ¶ 12.

432. The SOS Office then sent her another ballot for the June 2020 election that she had not requested, so she destroyed it, believing it to be an error. Opp. Ex. 231 ¶ 12; Opp. Ex. 230 at 118:14-119:9.

433. Ms. Price requested a ballot for the August 2020 election, but never received a ballot and does not know why. Dkt. 1599, Feb. 2023 Price Decl. ¶¶ 3-4; Opp. Ex. 230 at 118:14-119:9.

434. Ms. Price could not vote in the August 2020 election because she never received an absentee ballot and was not willing to vote using the BMD system, which she has no confidence in. Dkt. 1599, Feb. 2023 Price Decl. ¶ 3.

435. When the date of the Mary 24, 2020 primary changed, Ms. Price contacted DeKalb County because she was concerned her original ballot would not be counted. The County election office told her to fill out another application. She did so, but never received another absentee ballot. Opp. Ex. 231 ¶ 12.

436. The action of casting his own individual vote and personally exercising his constitutional right – and having confidence that his vote will be reliably counted—is paramount to Jeffrey Schoenberg. Opp. Ex. 232 ¶¶ 7-8.

437. Mr. Schoenberg would like to vote in person in future elections, because it is his preferred method of voting. Opp. Ex. 233 at 92:23.

438. However, he is concerned that he will be disenfranchised by Georgia’s current BMD voting system—that his vote will not be counted accurately, and nobody would even be able to tell after the fact. Opp. Ex. 235 ¶ 10.

439. Mr. Schoenberg is also concerned about the reliability of voting by absentee ballot in Georgia due to mail delays and problems obtaining ballots and having them counted when returned. Opp. Ex. 236 ¶ 12.

440. Mr. Schoenberg, therefore, decided to vote in-person in the 2020 Presidential Preference Primary, but found Georgia's BMD process so disturbingly unreliable that he planned to vote absentee thereafter. Opp. Ex. 233 at 132:16-133:16.

441. Mr. Schoenberg's experience voting absentee in a January 5, 2021, Public Service Commission/special run-off combination election confirmed his concerns that absentee ballots are also an unreliable way to cast a vote in Georgia. Opp. Ex. 232 ¶ 10; Opp. Ex. 233 at 94:12-95:3.

442. Mr. Schoenberg requested an absentee ballot for the January 5, 2021 election, received confirmation of his request, but never received the ballot, with no further communication. Opp. Ex. 232 ¶ 10; Opp. Ex. 233 at 94:12-95:3.

443. When he realized his ballot would likely not arrive in time, Mr. Schoenberg voted early in person on a Georgia BMD in January 2021. Opp. Ex. 232 ¶ 10; Opp. Ex. 233 at 94:12-95:3.

444. Although Mr. Schoenberg was able to make his selections on a Georgia BMD and scan his ballot in January 2021, he could not verify the

scannable portion of the ballot (the QR code) and left the polling place without confidence that his vote would be counted as cast. Opp. Ex. 232 ¶¶ 10-11.

445. Mr. Schoenberg feels that choosing between voting in-person or absentee in Georgia is akin to choosing “this poison rather the other.” Opp. Ex. 233 at 132:12-133:3; *see also* Opp. Ex. 236 ¶¶ 9-11.

446. Mr. Schoenberg’s vote is deeply personal and is a unique expression of his individual freedoms and his unique combination of values, beliefs, judgments, perspectives, and life experiences. Opp. Ex. 232 ¶¶ 7-8.

447. Another identical ballot would still differ from Mr. Schoenberg’s because what his vote represents to him and how he reached his exact selections is unique. Opp. Ex. 232 ¶ 8.

448. The loss of his vote would be a profound and personal harm to Mr. Schoenberg, regardless of the outcome of the election. Opp. Ex. 232 ¶ 8; Opp. Ex. 233 at 125:15-126:6.

449. Voting absentee deprives Mr. Schoenberg of the civic experience and his right to vote alongside his fellow citizens, something deeply important to Georgia voters as SOS Office COO Gabriel Sterling emphasized. Opp. Ex. 236 ¶ 10; Opp. Ex. 237 (“[H]istorically, they do not like voting by mail in Georgia. Part of that has to do with the history of our state. Martin Luther King Jr. is from there. People have fought for the right to vote. They like the pageantry of it. They like going to see their neighbors in line. It’s something that helps their heart.”).

450. On the other hand, voting on Georgia’s BMDs would risk disenfranchisement for Mr. Schoenberg. Opp. Ex. 236 ¶ 10.

451. Mr. Schoenberg described verifying the printed text on his Georgia BMD ballot as “a silly thing to do” because what he was reading is not what the machine would read. Opp. Ex. 233 at 98:3-13.

452. It is troubling for Mr. Schoenberg that the lessons he teaches his daughters about the importance of exercising citizenship rights are undercut by the reality that he cannot have faith in Georgia elections due to the failings with its BMD system. Opp. Ex. 238 ¶ 9.

453. Mr. Schoenberg would be satisfied with any voting system that the public and the state can verify is reliable, transparent, and verifiable. Opp. Ex. 233 at 37:15-23.

454. Mr. Schoenberg believes that hand-marked ballots are not the only system that could be reliable, transparent, and verifiable. Opp. Ex. 233 at 37:15-23.

455. During every Georgia election since 2006, Mr. Schoenberg has thought casting his vote could be a “hollow exercise” because no one could know whether his vote was recorded, tallied, or reporting correctly using the DREs and then Georgia’s BMDs. Opp. Ex. 238 ¶ 7.

456. After he voted on a Georgia BMD, Mr. Schoenberg left the polling place without any certainty that he had meaningfully participated in the election. Opp. Ex. 233 at 135:8-18.

457. If Georgia's BMDs were prohibited going forward, Mr. Schoenberg would perceive less risk while voting. Opp. Ex. 235 ¶ 11; Opp. Ex. 236 ¶.

458. Mr. Schoenberg also has concerns that Georgia's BMD system is flawed because it cannot be properly audited. Opp. Ex. 233 at 83:25-84:2.

459. There is no record to tell Mr. Schoenberg that elections conducted with Georgia's BMD system are properly counted and that his vote particularly gets counted as cast. Opp. Ex. 233 at 84:2-4.

460. Mr. Schoenberg does not know if his vote on Georgia's BMD system in the January 5, 2021 election reflected his vote as cast or was counted at all. Opp. Ex. 232 ¶ 12; Opp. Ex. 233 at 135:8-18.

461. Every time Mr. Schoenberg votes on a system that is not reasonably secure, he cannot know that he has participated in the democratic process. Opp. Ex. 233 at 125:3-126:6.

462. A court order prohibiting Georgia's BMDs and requiring hand-marked paper ballots would allow Mr. Schoenberg to verify his vote was cast as intended and would be counted as cast. Opp. Ex. 235 ¶¶ 10-11; Opp. Ex. 236 ¶ 10.

463. There have been changes in Georgia law that make it more difficult to vote absentee, and therefore harder to vote on a hand-marked paper ballot. Opp. Ex. 105 at 289:13-25.

464. Voter confidence in election systems is important. Opp. Ex. 105 at 296:9-17; Opp. Ex. 48 at 79:5-15.

465. Suppressing even a relatively small handful of votes, particularly in a local election with a small number of voters, could be enough to change the outcome of an election. Opp. Ex. 29 at 209:9-14 (Payton testimony).

O. It is Feasible to Implement a Voting System Using Hand-Marked Paper Ballots in Georgia.

466. Experts consider the use of hand-marked paper ballots (“HMPBs”) for all in-person voters (with exceptions for voters with specific accessibility needs) to be the gold standard for elections systems. *See, e.g.*, Opp. Ex. 26 at 103:3-5 (testimony of Dr. Alex Halderman); Opp. Ex. 152 at 2; Opp. Ex. 99 at PDF p. 46, ¶ 18; Opp. Ex. 239 ¶ 21.

467. Georgia could transition swiftly and cost-effectively to HMPBs, as the primary elements for a HMPB system are already in place. *See, e.g.*, Opp. Ex. 240

at 19; Opp. Ex. 54 ¶ 24; Opp. Ex. 56 at 137:14-138:15; Opp. Ex. 44 at 227:13-228:22; *see also* Opp. Ex. 2 at 148 (directing State Defendants to include hand-marked paper ballots in the default plan they were directed to prepare during the rollout of the BMD system).

468. A HMPB-based voting system in Georgia would require far less equipment and employees than Georgia’s current BMD-based system because counties would no longer require clunky, complicated, costly machines or printer stations. Opp. Ex. 29 at 157:9-15.

469. The Georgia Election Code authorizes superintendents to adopt HMPBs instead of Georgia’s BMDs on an emergency basis where the use of the BMDs for any reason is not practicable. O.C.G.A. §§ 21-2-281, 21-2-334.

470. Georgia law already requires polling places to print enough HMPBs for all voters “in the event of an emergency.” State Election Board Rule 183-1-12-.11(2)(c)-(d).

471. Georgia's Election Code provides the elections supervisor with discretion over the existence of an emergency situation. State Election Board Rule 183-1-12-.11(2)(c)-(d).

472. The Dominion ICP scanners used in Georgia's BMD system statewide already have the capability to count barcode or HMPBs interchangeably. Opp. Ex. 54 ¶ 4; Opp. Ex. 54 ¶¶ 4, 37-40; Opp. Ex. 56 at 128:23-129:22; *see also* Opp. Ex. 2 at 146 ("scanning technology provided by Dominion under the State's contract and funds authorized in connection with HB 316" could be used to implement a constitutionally-acceptable HMPB voting system).

473. Because Georgia already has the ability to print and tabulate HMPBs on a widespread scale, there is minimal additional burden associated with moving to HMPBs statewide. *See, e.g.*, Opp. Ex. 240 at 19; Opp. Ex. 54 ¶ 24; Opp. Ex. 56 at 137:14-138:15; Opp. Ex. 105 at 218:13-219:3; *see also* Opp. Ex. 2 at 146 (finding that the "scanning technology provided by Dominion under the State's contract and funds authorized in connection with HB 316" could be used to implement a constitutionally-acceptable hand-marked paper ballot voting system).

474. Election workers would require little or no new technical training for an HMPB system in Georgia because paper ballots make use of the same equipment, and election workers are already trained on the use of paper ballots because they must be prepared to use them in exigent circumstances. Opp. Ex. 44 at 336:7-10.

475. Under Georgia's current BMD-based voting system, for every election, numerous county and contract employees take tens of thousands of heavy BMD touchscreens, BMD printers, and BMD backup batteries out of storage and transport them to polling places, set up, program, test, maintain, and secure that equipment, and, after the election, dismantle the equipment and transport it back to storage. Opp. Ex. 193 at 23:7-29:3; 33:3-34:20.

476. A system using primarily HMPBs would be much less expensive than Georgia's current BMD system because it would require less equipment production, upkeep, personnel, and delivery. Opp. Ex. 29 at 157:9-15.

P. State Law Requires Fulton County to Conduct Elections and Implement the Voting System in Fulton County.

477. Fulton Defendants must, under State law, conduct elections and thereby implement the voting system in Fulton County. O.C.G.A. § 21-2-70; Dkt. 1573 p. 13-14.

478. Fulton Defendants had knowledge of security failures in Georgia's voting system, including some of Dr. Halderman's statements about vulnerabilities in the BMD system. Opp. Ex. 70 at 165:4-166:4, 166:25-167:10; Opp. Ex. 243; Opp. Ex. 244; Opp. Ex. 245; Opp. Ex. 246; *see also* Dkt. 1590-10.

479. Fulton Defendants expressed "serious concerns" in 2020 that "the new voting system is failing to read all votes marked by voters on absentee by mail ballots." Opp. Ex. 247 at 2.

480. Fulton County's Elections Director, Richard Mr. Barron, has admitted that there is "no way for the voter to verify" the QR code on the BMD-printed ballot. Opp. Ex. 70 at 18:10-11, 31:1-5, 173:13, 180:20-181:7. He also testified: "the best thing to do would be for there to be minimal barcodes or Q.R. codes." Opp. Ex. 70 at 181:20-183:4.

481. Fulton Defendants have not assessed or examined the Georgia voting system for cyber-attack vulnerabilities. Opp. Ex. 63 at 100:21-25.

482. As of January 21, 2022, Fulton Defendants were not taking any measures to eliminate or remediate any cyber-attack vulnerabilities in the Georgia voting system. Opp. Ex. 63 at 101:1-6.

483. Mr. Gilstrap was not aware of efforts that Fulton Defendants must make to ensure that components of Georgia's voting system as used in Fulton County are actually air gapped. Opp. Ex. 63 at 17:19-22.

484. Mr. Gilstrap was not aware of claims that someone made a successful hacking attempt into Fulton County voting machines via remote Wi-Fi towards the end of 2020. Opp. Ex. 63 at 102:13-18.

485. It would be a concern to Fulton County if a third party had taken copies or images of voting equipment used in Fulton County elections, or voting data in those elections. Opp. Ex. 63 at 122:23-123:8.

486. Dominic Olomo was unable to answer what process Fulton County would follow if it learned about a problem with a Georgia BMD. Opp. Ex. 167 at 22:15-21; 23:10-23.

487. Mr. Olomo was not able to testify about wireless connections involving components of Georgia's voting system apart from stating that poll pads are connected to Wi-Fi during bulk updates and during logic and accuracy testing. Opp. Ex. 167 at 29:12-30:5.

488. Fulton County has not conducted an assessment as to whether the information on cards created by poll pads and then inserted into Georgia BMDs as part of the voter check-in system are vulnerable to malicious attacks. Opp. Ex. 70 at 41:24-42:11.

489. Mr. Olomo stated there were no policies concerning cybersecurity (i.e., protection against cyber-attack vulnerabilities) that come to Fulton County from the Secretary of State's office and that Fulton County did not have any such policies of its own. Opp. Ex. 167 at 36:23-37:5.

490. Mr. Olomo had not read any of the expert reports in the case and was otherwise not aware of them. Opp. Ex. 167 at 33:12-19.

491. There were operational or execution issues and challenges for Georgia's election system in the Fulton County June 2020 primary election, including unavailability of emergency paper ballots. Opp. Ex. 63 at 131:10-132:12; Opp. Ex. 111.

492. One issue encountered in the Georgia primary runoff election in 2020 was a problem with poll pad "decoders," which prevented the printing of ballot access cards. Problems such as the decoder issue have occurred since the August 2020 election in Georgia. Opp. Ex. 63 at 134:19-138:16; Opp. Ex. 112.

493. One issue encountered in 2020 elections was Georgia BMDs printing ballots with two QR codes, an issue that had previously been discovered during logic and accuracy testing. Opp. Ex. 63 at 138:21-141:15; Opp. Ex. 248.

494. Despite the issue of Georgia BMDs printing ballots with two QR codes, Fulton Defendants did not seek to alter or change their logic and accuracy procedures. Opp. Ex. 63 at 141:16-142:2.

495. Neither Fulton Defendants nor anyone at their direction or behest scans or conducts other inspections of USB devices used to update the software on Georgia's BMDs. Opp. Ex. 70 at 34:5-14.

496. Neither Fulton Defendants nor anyone at their direction or behest has conducted an assessment as to whether the information on cards created by poll pads and then inserted into Georgia BMDs as part of the voter check-in system are vulnerable to malicious attacks. Opp. Ex. 70 at 41:24-42:11.

497. Fulton County has an adversarial relationship with the Georgia Secretary of State and his office as well as the State Election Board. Opp. Ex. 70 at 115:25-117:14.

Respectfully submitted this 13th day of February, 2023.

/s/ David D. Cross
David D. Cross (*pro hac vice*)
Mary G. Kaiser (*pro hac vice*)
Hannah R. Elson (*pro hac vice*)
MORRISON & FOERSTER LLP
2100 L Street, NW, Suite 900
Washington, DC 20037
(202) 887-1500

/s/ Halsey G. Knapp, Jr.
Halsey G. Knapp, Jr.
GA Bar No. 425320
Adam M. Sparks
GA Bar No. 341578
KREVOLIN & HORST, LLC
1201 West Peachtree Street, NW
Suite 3250
Atlanta, GA 30309
(404) 888-9700

Counsel for Plaintiffs Donna Curling, Donna Price & Jeffrey Schoenberg

/s/ Bruce P. Brown

Bruce P. Brown
Georgia Bar No. 064460
BRUCE P. BROWN LAW LLC
1123 Zonolite Rd. NE
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

/s/ Robert A. McGuire, III

Robert A. McGuire, III
Admitted Pro Hac Vice
(ECF No. 125)
ROBERT MCGUIRE LAW FIRM
113 Cherry St. #86685
Seattle, Washington 98104-2205
(253) 267-8530

/s/ Russell T. Abney

Russell T. Abney
Georgia Bar No. 000875
WATTS GUERRA, LLP
4 Dominion Drive, Building 3
Suite 100
San Antonio, TX 78257
(404) 670-0355

Counsel for Plaintiff Coalition for Good Governance

/s/ Cary Ichter

Cary Ichter
Georgia Bar No. 382515
ICHTER DAVIS LLC
3340 Peachtree Road NE
Suite 1530
Atlanta, Georgia 30326
(404) 869-7600

*Counsel for Plaintiffs William Digges III, Laura Digges,
Ricardo Davis & Megan Missett*

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRAD RAFFENSPERGER, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

CERTIFICATE OF COMPLIANCE

Pursuant to LR 7.1(D), I hereby certify that the foregoing document has been prepared in accordance with the font type and margin requirements of LR 5.1, using font type of Times New Roman and a point size of 14.

/s/ David D. Cross
David D. Cross

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRAD RAFFENSPERGER , ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

CERTIFICATE OF SERVICE

I hereby certify that on February 13, 2023, a copy of the foregoing **CORRECTED JOINT STATEMENT OF ADDITIONAL FACTS IN SUPPORT OF PLAINTIFFS' OPPOSITIONS TO DEFENDANTS' MOTIONS FOR SUMMARY JUDGMENT** was electronically filed with the Clerk of Court using the CM/ECF system, which will automatically send notification of such filing to all attorneys of record.

/s/ David D. Cross
David D. Cross