

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual;)
)
COALITION FOR GOOD)
GOVERNANCE, a non-profit corporation)
organized and existing under Colorado)
Law;)
)
DONNA PRICE, an individual;)
)
JEFFREY SCHOENBERG, an individual;)
)
LAURA DIGGES, an individual;)
)
WILLIAM DIGGES III, an individual;)
)
RICARDO DAVIS, an individual;)
)
Plaintiffs,)
)
v.)
)
BRIAN P. KEMP, in his individual)
capacity and his official capacity as)
Secretary of State of Georgia and)
Chair of the STATE ELECTION BOARD;)
)
DAVID J. WORLEY, REBECCA N.)
SULLIVAN, RALPH F. "RUSTY")
SIMPSON, and SETH HARP, in their)
individual capacities and their official)
capacities as members of the STATE)
ELECTION BOARD;)
)
THE STATE ELECTION BOARD;)
)
RICHARD BARRON, in his individual)
capacity and his official capacity as)

CIVIL ACTION
FILE NO.: 2017cv292233

DEMAND FOR
JURY TRIAL

Director of the FULTON COUNTY)
BOARD OF REGISTRATION AND)
ELECTIONS;)

MARY CAROLE COONEY, VERNETTA)
NURIDDIN, DAVID J. BURGE, STAN)
MATARAZZO and AARON JOHNSON)
in their individual capacities and official)
capacities as members of the FULTON)
COUNTY BOARD OF REGISTRATION)
AND ELECTIONS;)

THE FULTON COUNTY BOARD OF)
REGISTRATION AND ELECTIONS;)

MAXINE DANIELS, in her individual)
capacity and her official capacity as)
Director of VOTER REGISTRATIONS)
AND ELECTIONS FOR DEKALB)
COUNTY;)

MICHAEL P. COVENY, ANTHONY)
LEWIS, LEONA PERRY, SAMUEL)
E. TILLMAN, and BAOKY N. VU)
in their individual capacities and official)
capacities as members of the DEKALB)
COUNTY BOARD OF REGISTRATIONS)
AND ELECTIONS;)

THE DEKALB COUNTY BOARD OF)
REGISTRATIONS AND ELECTIONS;)

JANINE EVELER, in her individual)
capacity and her official capacity as)
Director of the COBB COUNTY)
BOARD OF ELECTIONS AND)
REGISTRATION;)

PHIL DANIELL, FRED AIKEN, JOE)
PETTIT, JESSICA BROOKS, and)

DARRYL O. WILSON in their individual)
capacities and official capacities as)
members of the COBB COUNTY)
BOARD OF ELECTIONS AND)
REGISTRATION;)
))
THE COBB COUNTY BOARD OF)
ELECTIONS AND REGISTRATION;)
))
MERLE KING, in his individual capacity)
and his official capacity as Executive)
Director of the CENTER FOR ELECTION)
SYSTEMS AT KENNESAW STATE)
UNIVERSITY; and)
))
THE CENTER FOR ELECTION)
SYSTEMS AT KENNESAW STATE)
UNIVERSITY)
))
Defendants.)

PLAINTIFFS’ MOTION FOR LEAVE TO FILE AMENDED COMPLAINT

COME NOW, Plaintiffs in the above-styled case to respectfully move this Court to grant them leave to amend their **Verified Complaint for Declaratory Relief, Injunctive Relief, and Writ of Mandamus** (“Original Complaint”) by filing their **Verified Amended Election Contest and Complaint for Declaratory Relief, Injunctive Relief, Damages, and Writs of Mandamus** (“Amended Complaint”), attached as Exhibit A (“Motion”). Furthermore, for the reasons described below, Plaintiffs respectfully request that this Court either grant Plaintiffs’ Motion without further briefing or set an expedited briefing schedule.

I. Statement of Facts

1. On July 3, 2017, Plaintiffs filed their Complaint with this Court. The Original Complaint contains the following claims related to the June 20, 2017 Runoff Election between Karen Handel and Thomas Jonathan “Jon” Ossoff for Georgia’s 6th Congressional District (“Runoff”) and Georgia’s unconstitutional and illegal ballots and election system:

1. A claim under Article II, Paragraph 1 of the Georgia Constitution for declaratory and injunctive relief based on plaintiffs’ rights to have elections “conducted in accordance with procedures provided by law”;
2. A due process claim pursuant to 42 U.S.C. § 1983 for declaratory and injunctive relief;
3. An equal protection claim pursuant to 42 U.S.C. § 1983 for declaratory and injunctive relief;
4. An election contest of the Runoff pursuant to O.C.G.A. § 21-2-520 *et seq.*, seeking declaratory and injunctive relief based on misconduct and irregularities in employing an unsecure, uncertified voting system;
5. An election contest of the Runoff pursuant to O.C.G.A. § 21-2-520 *et seq.* seeking declaratory and injunctive relief based on misconduct and irregularities in using illegal ballots;
6. A claim for declaratory and injunctive relief based on certain Defendants’ failure to recanvass votes upon requests pursuant to Ga. Comp. R. & Regs. 183-1-12;
7. A claim for declaratory and injunctive relief based on certain Defendants’ failure to approve Georgia’s voting system pursuant to O.C.G.A. 21-2-379.2 and failure to certify the voting system pursuant to Ga. Comp. R. & Regs. 590-8-1-.01; and

8. A claim for a writ of mandamus requiring Secretary of State Brian Kemp to reexamine Georgia's voting system pursuant to O.C.G.A. § 21-2-379.2(b).

2. Pursuant to election contest procedures, the Complaint was due to be filed within 5 court days of the certification of the election, which occurred on June 26, 2017, leaving little time to work out the many details of Plaintiffs' extensive Complaint.

3. The Complaint is in various stages of service, with no responsive pleadings having yet been filed.

4. Plaintiffs hereby seek to make the following changes to its claims by filing the Amended Complaint:

1. Adding as a Defendant Mr. Mark Wingate, who recently became a member of the Fulton County Board of Registration and Elections;
2. Adding an additional mandamus claim against the Defendant members of State Board, the State Board, Daniels, members of the DeKalb Board, DeKalb Board, Eveler, members of the Cobb Board, Cobb Board, Barron, members of the Fulton Board, and Fulton Board, in their Official Capacities to require the use of legally compliant voting mechanisms in future elections;
3. Removing the Center for Election Services from the caption and as a referenced party; those claims remain against its Executive Director, Merle King, in the Amended Complaint;
4. Revising the relief sought to include nominal damages, attorneys' fees and costs, and modified declaratory and injunctive relief;
5. Removing the Defendants Barron and the members of the Fulton County Board of Registration and Elections from Plaintiff Coalition for Good Governance's claim for declaratory and injunctive relief

based on certain Defendants' failure to recanvass votes upon requests pursuant to Ga. Comp. R. & Regs. 183-1-12;

6. Revising the capacity in which individuals have been sued with respect to certain claims:
 - Removing election contest claims against Defendants in their individual capacities (retaining those claims against Defendants only in their official capacities);
 - Adding Plaintiffs' two 42 U.S.C. § 1983 claims against all individual Defendants in their individual capacities (in addition to the same claims against them in their official capacities)
7. Adding additional exhibits, including a declaration and an additional affidavit;
8. Revising language, fixing typos, including additional authority, modifying allegations, and changing the order of the claims;
9. Adding a section under the caption to indicate the names of the candidates involved in the election contest.

II. Argument and Citation to Supporting Authority

Although Plaintiffs may usually amend a pleading “as a matter of course and without leave of court at any time before entry of a pretrial order” (O.C.G.A. § 9-11-15(a)), this case includes election contest claims, which are governed by special procedures. For election contest claims, the Georgia Code states that, “[a]fter filing, any petition ... may be amended with leave of the court so as to include the specification of additional grounds of contest, other relevant facts, or prayer for further relief.” O.C.G.A. § § 21-2-524(g). Since this action includes both election-

contest claims and non-election-contest claims, Plaintiffs have, in an abundance of caution, sought leave of the court to amend its entire Complaint.

Here, Plaintiffs wish to revise and supplement their factual allegations, adjust their claims, and pray for further relief as listed above. They respectfully request this Court grant them leave to do so.

Additionally, Plaintiffs wish to add a new party in their Amended Complaint. Plaintiffs request that the Court permit them to do so. Georgia Code section § 9-11-21 provides, “Parties may be dropped or added by order of the court on motion of any party... on such terms as are just.” Here, Mr. Wingate recently became a member of the Fulton County Board of Registration and Elections (on information and belief, this happened on July 1, 2017—two days before the Complaint was filed). Mr. Wingate thereby became responsible for the election systems that are at issue in this case and for which Plaintiffs seek, *inter alia*, injunctive and declaratory relief. Accordingly, Plaintiffs respectfully request that the Court permit them to add Mr. Wingate as a defendant in this case.

III. Conclusion

For the above-stated reasons, Plaintiffs respectfully request that this Court grant its Motion and grant them leave to file their Amended Complaint, attached hereto, in accordance with O.C.G.A. § 21-2-524(g), O.C.G.A. § 9-11-15(a), and O.C.G.A. § 9-11-21. Because this matter includes an election contest, Plaintiffs

understand that the matter is to be handled with all due expediency. See O.C.G.A. 21-2-524 et seq. For that reason and because the Amended Complaint constitutes an early and non-controversial refining of its claims, Plaintiffs respectfully request that this Motion be granted without the need for a briefing from Defendants or, if it deems briefing necessary, that the Court set an expedited briefing schedule.

This 4th day of August 2017.

/s/ Bryan Ward
Bryan Ward, Esq.
Georgia Bar No. 736656
Marvin Lim, Esq.
Georgia Bar No. 147236
Holcomb + Ward LLP
3399 Peachtree Rd NE, Suite 400
Atlanta, GA 30326
(404) 601-2803 (office)
(404) 393-1554 (fax)
Bryan.Ward@holcombward.com
Marvin@holcombward.com

EXHIBIT 1

**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual;)

)

COALITION FOR GOOD)

GOVERNANCE, a non-profit corporation)

organized and existing under Colorado)

Law;)

)

DONNA PRICE, an individual;)

)

JEFFREY SCHOENBERG, an individual;)

)

LAURA DIGGES, an individual;)

)

WILLIAM DIGGES III, an individual;)

)

RICARDO DAVIS, an individual;)

)

Plaintiffs,)

)

v.)

)

CIVIL ACTION

FILE NO.: 2017CV292233

BRIAN P. KEMP, in his individual)

capacity and his official capacity as)

Secretary of State of Georgia and)

Chair of the STATE ELECTION BOARD;)

**DEMAND FOR
JURY TRIAL**

)

DAVID J. WORLEY, REBECCA N.)

SULLIVAN, RALPH F. "RUSTY")

SIMPSON, and SETH HARP, in their)

individual capacities and their official)

capacities as members of the STATE)

ELECTION BOARD;)

THE STATE ELECTION BOARD;

RICHARD BARRON, in his individual capacity and his official capacity as Director of the FULTON COUNTY BOARD OF REGISTRATION AND ELECTIONS;

MARY CAROLE COONEY, VERNETTA NURIDDIN, DAVID J. BURGE, STAN MATARAZZO, AARON JOHNSON, and MARK WINGATE, in their individual capacities and official capacities as members of the FULTON COUNTY BOARD OF REGISTRATION AND ELECTIONS;

THE FULTON COUNTY BOARD OF REGISTRATION AND ELECTIONS;

MAXINE DANIELS, in her individual capacity and her official capacity as Director of the DEKALB COUNTY BOARD OF REGISTRATION AND ELECTIONS;

MICHAEL P. COVENY, ANTHONY LEWIS, LEONA PERRY, SAMUEL E. TILLMAN, and BAO KY N. VU in their individual capacities and official capacities as members of the DEKALB COUNTY BOARD OF REGISTRATION AND ELECTIONS;

THE DEKALB COUNTY BOARD OF)
REGISTRATION AND ELECTIONS;)

JANINE EVELER, in her individual)
capacity and her official capacity as)
Director of the COBB COUNTY)
BOARD OF ELECTIONS AND)
REGISTRATION;)

PHIL DANIELL, FRED AIKEN, JOE)
PETTIT, JESSICA BROOKS, and)
DARRYL O. WILSON in their individual)
capacities and official capacities as)
members of the COBB COUNTY)
BOARD OF ELECTIONS AND)
REGISTRATION;)

THE COBB COUNTY BOARD OF)
ELECTIONS AND REGISTRATION;)

MERLE KING, in his individual capacity)
and his official capacity as Executive)
Director of the CENTER FOR ELECTION)
SYSTEMS AT KENNESAW STATE)
UNIVERSITY; and)

Defendants.)

KAREN HANDEL and)
THOMAS JONATHAN OSSOFF)

Candidates in Contested Election.)

**VERIFIED AMENDED ELECTION CONTEST AND
COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF,
DAMAGES, AND WRITS OF MANDAMUS**

COMES NOW, Plaintiffs, named above, to show this Honorable Court the following for their Complaint against the above-named Defendants:

I. INTRODUCTION

Georgia’s 6th Congressional District voters can never know who was legitimately elected on June 20, 2017 to become their Representative to the 115th United States Congress. They know only the output of an undeniably compromised voting system that—according to Plaintiffs and many of the nation’s most qualified experts—generated a result that cannot reasonably be relied upon. To declare that result to be will of the voters—as Defendants have done—is to engage in farce.

The high-profile June 20, 2017 Runoff Election between Karen Handel and Thomas Jonathan “Jon” Ossoff for Georgia’s 6th Congressional District (“Runoff”) took place in an environment in which sophisticated hackers—whether Russian or otherwise—had the capability and intent to manipulate elections in the United States. These hackers not only had the capability, but they also had easy access. From at least August 2016 through early March 2017, all the computer files that a bad actor would need to manipulate the Runoff and all of Georgia’s elections—including tabulation database programs, voting system passwords,

programs used to create voting machine memory cards, and voter registration information—were left out in the open on the internet, without requiring so much as a password to obtain. Without solving these known issues, Defendants willfully conducted the Runoff almost entirely on illegal, unverifiable electronic ballots for which discrepancies cannot be corrected, providing perfect cover for electronic manipulation.

The speculative nature of the Runoff’s purported result was caused by Defendants’ willful violation of numerous mandatory requirements of Georgia’s Election Code, O.C.G.A. Title 21, Chapter 2 (“Election Code”). These requirements prohibited the use of the voting systems that were employed and the resulting certification of their results. Furthermore, Defendants abridged electors’ statutory rights of recanvass—rights the electors invoked to attempt to address suspected irregularities in the post-election process prior to the certification of the election results.

This action seeks to set aside the purported result of the Runoff to ensure that 6th Congressional District electors have the free and fair elections to which they are entitled pursuant to the federal Constitution, federal statutory civil rights law, the Georgia Constitution, Georgia statutory law, and Georgia regulations governing elections. It also seeks injunctive relief to ensure that upcoming elections meet statutory and constitutional guarantees.

II. PARTIES

A. PLAINTIFFS

1.

Plaintiff DONNA CURLING (“Curling”) is an elector of the State of Georgia and a resident of Fulton County and the 6th Congressional District of the State of Georgia. Curling is a member of the COALITION FOR GOOD GOVERNANCE. Curling is a Georgia elector who requested that Secretary of State Brian P. Kemp (“Secretary Kemp”) reexamine Georgia’s Voting System.¹ Curling is an “aggrieved elector who was entitled to vote” for a candidate in the Runoff under Georgia Code Section 21-2-521. Furthermore, the Optical Scanning System² under which she cast her vote substantially burdens her right to vote as the system was fundamentally insecure during the Runoff, is not compliant with applicable statutes, and cannot be reasonably relied upon to have properly recorded and counted her vote or the votes of other electors. Curling experienced considerable inconvenience to cast her vote by paper absentee ballot so as to ensure that her vote was permanently recorded on an independent record that could be recounted in an election contest and to avoid the risk of voting on non-

¹ “Georgia’s Voting System” is defined below in Section IV.B.1, ¶ 55. Georgia’s Voting System includes both a DRE system and an optical scanning system that share certain underlying components but are governed by separate statutory schemes, as discussed below.

² “Optical Scanning System” is defined below in Section IV.B.1, ¶¶ 55; 59 – 60.

compliant Direct Recording Electronic (“DRE”) machines used in Georgia’s DRE System.³ Curling intends to vote in the upcoming November municipal elections in the City of Roswell and wishes to vote in her neighborhood precinct on election day. Without the intervention of this Court, Curling will be forced to cast her ballots under a system that substantially burdens her right to vote as Georgia’s Voting System is fundamentally insecure, illegally employed, and cannot be reasonably relied upon to record and count properly her votes or the votes of other electors. As such, she has standing to bring her claims.

2.

Plaintiff COALITION FOR GOOD GOVERNANCE (“CGG”) (formerly Rocky Mountain Foundation) is a non-profit corporation organized and existing under the laws of the State of Colorado. CGG’s purpose is to advance the constitutional liberties and individual rights of citizens, with an emphasis on elections. CGG is a membership organization and its membership includes Curling, Donna Price, Ricardo Davis, and other electors of the State of Georgia who reside in, variously, Fulton County, Cobb County, DeKalb County, the 6th Congressional District of the State of Georgia, and various municipalities that will conduct elections in November 2017. Several of CGG’s Georgia elector members voted in the Runoff, with some using the DRE System and some using the Optical

³ “DRE System” is defined below in Section IV.B.1, ¶¶ 55 – 57.

Scanning System. Depending on the method of voting, members were subjected to a system that provided unequal treatment and differing weights to their votes and that abridged their rights to canvass.

3.

Plaintiff CGG has associational standing to bring this complaint on behalf of CGG's Georgia individual elector members because (1) those members would otherwise have standing to sue in their own right; (2) the interests CGG seeks to protect are germane to CGG's purpose; and because (3) with the exception of Counts VI and VII, the relief requested herein does not require the participation of CGG's individual Georgia elector members in the lawsuit.

4.

Plaintiff DONNA PRICE ("Price") is an elector of the State of Georgia and a resident of DeKalb County. Price is a Georgia elector who requested that Secretary Kemp reexamine Georgia's Voting System. She plans to vote in all future elections for which she is an eligible elector. Without the intervention of this Court, Price will be forced to cast her ballots under a system that substantially burdens her right to vote as Georgia's Voting System is fundamentally insecure, illegally employed, and cannot be reasonably relied upon to record and count properly her votes or the votes of other electors. As such, she has standing to bring her claims.

5.

Plaintiff JEFFREY SCHOENBERG (“Schoenberg”) is an elector of the State of Georgia and a resident of DeKalb County and the 6th Congressional District of the State of Georgia. Schoenberg is an “aggrieved elector who was entitled to vote” for a candidate in the Runoff under O.C.G.A. § 21-2-521. Furthermore, the DRE System under which he cast his vote substantially burdens his right to vote as the system is fundamentally insecure, illegally employed, and cannot be reasonably relied upon to have recorded and counted properly his vote or the votes of other electors. He is a registered elector in the City of Dunwoody and plans to vote in the November 2017 municipal election. Without the intervention of this Court, Schoenberg will be forced to cast his ballots under a system that substantially burdens his right to vote as Georgia’s Voting System is fundamentally insecure, illegally employed, and cannot be reasonably relied upon to record and count properly his votes or the votes of other electors. As such, he has standing to bring his claims.

6.

Plaintiff LAURA DIGGES (“L. Digges”) is an elector of the State of Georgia and a resident of Cobb County and the 6th Congressional District of the State of Georgia. L. Digges is an “aggrieved elector who was entitled to vote” for a candidate in the Runoff under Georgia Code Section 21-2-521. Furthermore, the

Optical Scanning System under which she cast her vote substantially burdens her right to vote as the system is fundamentally insecure, not compliant with applicable statutes, and cannot be reasonably relied upon to have recorded and counted properly her vote or the votes of other electors. L. Digges experienced considerable inconvenience to cast her vote by paper absentee ballot to ensure that her vote was permanently recorded on an independent record that could be recounted in an election contest. L. Digges plans to vote in all future elections in which she is eligible. Without the intervention of this Court, L. Digges will be forced to cast her ballots under a system that substantially burdens her right to vote as Georgia's Voting System is fundamentally insecure, illegally employed, and cannot be reasonably relied upon to record and count properly her votes or the votes of other electors. As such, she has standing to bring her claims.

7.

Plaintiff WILLIAM DIGGES III ("W. Digges") is an elector of the State of Georgia and a resident of Cobb County and the 6th Congressional District of the State of Georgia. W. Digges is an "aggrieved elector who was entitled to vote" for a candidate in the Runoff under Georgia Code Section 21-2-521. Furthermore, the Optical Scanning System under which he cast his vote substantially burdens his right to vote as the system is fundamentally insecure, not compliant with applicable statutes, and cannot be reasonably relied upon to have recorded and counted

properly his vote or the votes of other electors. W. Digges experienced considerable inconvenience to cast his vote by paper absentee ballot to avoid the risk of a DRE ballot and ensure that his vote was permanently recorded on an independent record that could be recounted in an election contest. W. Digges plans to vote in all future elections in which he is eligible. Without the intervention of this Court, W. Digges will be forced to cast his ballots under a system that substantially burdens his right to vote as Georgia's Voting System is fundamentally insecure, illegally employed, and cannot be reasonably relied upon to record and count properly his votes or the votes of other electors. As such, he has standing to bring his claims.

8.

Plaintiff RICARDO DAVIS ("Davis") is an elector of the State of Georgia and a resident of Cherokee County. Davis is a Georgia elector who requested that Secretary Kemp reexamine Georgia's Voting System. Davis plans to vote in all future elections in which he is eligible. Without the intervention of this court, Davis will be forced to cast his ballots under a system that substantially burdens his right to vote as Georgia's Voting System is fundamentally insecure, illegally employed, and cannot be reasonably relied upon to record and count properly his votes or the votes of other electors. As such, he has standing to bring his claims.

B. DEFENDANTS

9.

Defendant BRIAN P. KEMP (“Kemp” or “Secretary Kemp”) is the Secretary of State of Georgia and, in that role, is also Chair of the State Election Board. Secretary Kemp is and was, for the Runoff, responsible for the orderly and accurate administration of Georgia’s electoral processes. This responsibility includes the duty to approve the use of legally compliant voting systems and to conduct any reexaminations of Georgia’s DRE System and Optical Scanning System currently in use, upon request or at his own discretion. See O.C.G.A. § 21-2-379.2(a)-(c); O.C.G.A. § 21-2-368(a)-(c); O.C.G.A. § 21-2-50.

10.

Defendants DAVID J. WORLEY, REBECCA N. SULLIVAN, RALPH F. “RUSTY” SIMPSON, and SETH HARP (“Members of the State Election Board”) are members of the State Election Board in Georgia. As members, they are, and were for the Runoff, responsible for (1) promulgating rules and regulations to ensure the legality and purity of all elections, (2) investigating frauds and irregularities in elections, and (3) reporting election law violations to the Attorney General or appropriate district attorney. See O.C.G.A. § 21-2-31.

11.

Defendant STATE ELECTION BOARD (“State Board”) is, and was for the Runoff, responsible for (1) promulgating rules and regulations to ensure the legality and purity of all elections, (2) investigating frauds and irregularities in elections, and (3) reporting election law violations to the Attorney General or appropriate district attorney. See O.C.G.A. § 21-2-31.

12.

Defendant RICHARD BARRON (“Barron”) is the Director of the Fulton County Board of Registration and Elections. As such, he was responsible for conducting the April 18, 2017 Special Election for Georgia’s 6th Congressional District (“Special Election”) and Runoff in Fulton County and continues to have such responsibility for upcoming elections.

13.

Defendants MARY CAROLE COONEY, VERNETTA NURIDDIN, DAVID J. BURGE, STAN MATARAZZO, AARON JOHNSON and MARK WINGATE (“Members of Fulton County Board of Registration and Elections”) are members of the Fulton County Board of Registration and Elections, other than Stan Matarazzo, who, on information and belief, was a member of the Fulton County Board of Registration and Elections until he was replaced by Mark Wingate. As members, they (other than Mark Wingate) were responsible for

conducting the Special Election and Runoff in Fulton County, and they (other than Stan Matarazzo) continue to have such responsibility for future elections in Fulton County.

14.

Defendant FULTON COUNTY BOARD OF REGISTRATION AND ELECTIONS (“Fulton Board”) is and was, for the Special Election and the Runoff, responsible for conducting elections in Fulton County.

15.

Defendant MAXINE DANIELS (“Daniels”) is the Director of the DeKalb County Board of Registration and Elections for DeKalb County. As such, she is, and was for the Special Election and the Runoff, responsible for conducting the elections in DeKalb County.

16.

Defendants MICHAEL P. COVENY, ANTHONY LEWIS, LEONA PERRY, SAMUEL E. TILLMAN, and BAOKY N. VU (“Members of DeKalb County Board of Registration and Elections”) are members of the DeKalb County Board of Registration and Elections. As members, they were responsible for conducting the Special Election and Runoff in DeKalb County and continue to have such responsibility for future elections in DeKalb County.

17.

Defendant DEKALB COUNTY BOARD OF REGISTRATION AND ELECTIONS (“DeKalb Board”) is, and was for the Special Election and the Runoff, responsible for conducting elections in DeKalb County.

18.

Defendant JANINE EVELER (“Eveler”) is the Director of the Cobb County Board of Elections and Registration. As such, she is, and was for the Special Election and the Runoff, responsible for conducting the elections in Cobb County.

19.

Defendants PHIL DANIELL, FRED AIKEN, JOE PETTIT, JESSICA BROOKS, and DARRYL O. WILSON (“Members of Cobb County Board of Elections and Registration”) are members of the Cobb County Board of Elections and Registration. As members, they were responsible for conducting the Special Election and Runoff in Cobb County and continue to have such responsibility for future elections in Cobb County.

20.

Defendant COBB COUNTY BOARD OF ELECTIONS AND REGISTRATION (“Cobb Board”) is, and was for the Special Election and the Runoff, responsible for conducting elections in Cobb County.

21.

Defendant MERLE KING (“King”) is Executive Director of the Center for Election Systems at Kennesaw State University. As such, he was responsible for overseeing, managing, and securing the electronic election infrastructure for the State of Georgia, including portions of both the DRE System and the Optical Scanning System, and creating Georgia’s ballots used in both the Special Election and the Runoff. King is expected to have these responsibilities for the remainder of 2017 and some part of 2018.

C. CANDIDATES

22.

Candidate KAREN HANDEL (“Handel”) was certified the winner of the Runoff on June 26, 2017 and was sworn into the United States House of Representatives on that date. Under the provisions of Georgia Code Section 21-2-524(f), Handel is deemed to be a litigant in this action.

23.

Candidate THOMAS JONATHAN “JON” OSSOFF (“Ossoff”) was a candidate in the Runoff. Under the provisions of Georgia Code Section 21-2-524(f), Ossoff is deemed to be a litigant in this action.

III. JURISDICTION AND VENUE

24.

Plaintiffs bring claims under the United States Constitution, the Georgia Constitution, and the laws, rules, and regulations of the State of Georgia. This Court has jurisdiction based upon Georgia Code Sections 9-4-1 to -10 to grant declaratory relief; based on Georgia Code Sections 9-5-1 to -11 to grant injunctive relief; and based upon Georgia Code Sections 9-6-20 to -28 to grant relief by way of issuing writs of mandamus. The Fulton County Superior Court has jurisdiction to hear the election contest contained herein based upon Georgia Code Section 21-2-523. Id. (“A contest case governed by this article shall be tried and determined by the superior court of the county where [a] defendant resides.”)

25.

Venue in this Court is proper under Georgia Code Section 9-10-30 because Fulton County is the county of residence of at least one of the Defendants against whom substantial equitable relief is prayed. The principal office of the Secretary of State’s Elections Divisions is located at 2 Martin L. King Jr. Drive SE, Suite 1104, Atlanta, Fulton County, Georgia, 30334. As such, jurisdiction and venue are proper in this Court.

IV. FACTUAL BACKGROUND

A. Georgia's Voting System Was Breached and Its Systems Exposed for at Least Seven Months.

26.

In August of 2016 Logan Lamb (“Lamb”), a professional cybersecurity expert was curious about the Center for Election Systems at Kennesaw State University (“CES”), an entity, directed by King, that served as an agent for the Secretary of State, responsible for overseeing, maintaining, and securing the electronic election infrastructure for the state of Georgia. Lamb discovered that he was able to access key parts of Georgia’s electronic election infrastructure through CES’s public website on the internet, without so much as entering a password. (See, generally, Affidavit of Logan Lamb, June 30, 2017, attached as “Exhibit A.”)

27.

In accessing these election files, Lamb discovered numerous critical vulnerabilities. For one, CES, under King’s direction, had improperly configured its server and also failed to patch a security flaw, publicly known since 2014, that could execute, create, copy, modify, or delete anything on CES’ server. (See Exhibit A, ¶ 5.) These vulnerabilities allowed anyone to access the internal executable files and election information stored on CES’s servers such as the following:

- Global Election Management Systems (“GEMS”) server databases;

- Executable files;
- PDFs with instructions and passwords for election workers to sign in to a central server on Election Day; and
- a database containing registration records, including private, personally identifying information for the state’s voters.

(See *id.*, ¶4.) On information and belief, Lamb also discovered software files for the state’s electronic pollbooks and county election databases used to prepare paper and electronic ballots, tabulate votes, and produce summaries of vote totals.

28.

In addition, the documents Lamb discovered included training videos, at least one of which “instructed users to first download files from the elections.kennesaw.edu website, put those files on a memory card, and insert that card into their local county voting systems.” (Exhibit A, ¶11.) This would be a serious security concern, allowing malicious software to be uploaded to voting machines in Georgia simply through the public portal that Lamb had easily accessed.

29.

The files that Lamb discovered constituted everything a bad actor (such as a hacker) would need in order to interfere with the election and manipulate its outcome.

30.

It is unknown how long King had left this data exposed before Lamb discovered it.

31.

Lamb immediately alerted King to the serious security vulnerabilities that he had discovered, advising King that CES should “[a]ssume any document that requires authorization has already been downloaded without authorization.”

(Exhibit A, ¶5.)

32.

King did not remediate the vulnerabilities to secure CES’ system. (Exhibit A, ¶7.)

33.

Seven months after Lamb was able to access critical information concerning Georgia’s Voting System via CES’s publicly available website on the internet, another cybersecurity expert was able to do the same. On or about March 1, 2017, Chris Grayson (“Grayson”), a colleague of Lamb’s, discovered that King had not fixed all of the security issues identified by Lamb in August 2016. That is, from at least August of 2016 to March of 2017—a time period that overlapped with known attempts by Russia to hack elections in the United States—King left exposed for anyone on the internet to see and potentially manipulate: election-related

applications, passwords for the central server, and private voter registration records.⁴

34.

On information and belief, King had failed to patch the known security flaw from 2014 on CES' server despite the FBI's explicit recommendation that responsible parties "[e]nsure all software and applications ... are fully patched." (Email Brian D. Newby, Executive Director, Election Assistance Commission to Kemp et al., August 23, 2016, attached as "Exhibit B," p 5.)

35.

Lamb confirmed Grayson's findings. Lamb then determined that he was still able to download information he had accessed in August 2016, as well as new information, including more recent database files and passwords. (Exhibit A, ¶8.)

36.

On information and belief, when Lamb notified King of the issue in August 2016, King told him, "It would be best if you were to drop this now," and warned

⁴ Kim Zetter, Will the Georgia Special Election Get Hacked, Politico, June 14, 2017, <http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255> (last visited July 27, 2017).

that, if Lamb talked, “the people downtown, the politicians . . . would crush [him].”⁵

37.

This time, in March 2017, rather than notifying King directly, Grayson notified Andrew Green, a colleague and a faculty member at Kennesaw State University (“KSU”). (See email chain from Merle King to Stephen Gay, dated March 1, 2017, attached as “Exhibit C.”) Mr. Green then notified KSU’s University Information Technology Services (“UITS”) Information Security Office, which in turn notified King. (Id.) KSU’s UITS Information Security Office is not directly affiliated with CES. (See KSU UITS Information Security Office, “Incident Report,” April 18, 2017, attached as “Exhibit D.”)

38.

Within an hour of Grayson’s notification, the KSU UITS Information Security Office established a firewall to isolate CES’s server. (See Exhibit D, pp. 1-2.) King took no such action after Lamb’s notification in August 2016.

39.

The day after Grayson’s notification, the KSU UITS Information Security Office seized CES’s server to preserve evidence “for later analysis and handoff to

⁵ Kim Zetter, *Will the Georgia Special Election Get Hacked*, Politico, June 14, 2017, <http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255> (last visited July 27, 2017).

federal authorities.” (Exhibit D, p. 2.) King took no such action after Lamb’s notification in August 2016.

40.

Two days after Grayson’s notification, the FBI was alerted and took possession of the server. (See Exhibit D, p. 1.) King took no such action after Lamb’s notification in August 2016.

41.

The KSU UITIS Information Security Office physically removed the backup server. (See Exhibit D.) King took no such action after Lamb’s notification in August 2016.

42.

The KSU UITIS Information Security Office also noted the presence of a wireless access point in the CES facility and live access to an external network in the private network closet. (See Exhibit D, pp. 3 – 4.)

43.

Although system security was a key responsibility of King and CES, the “Incident Report” also found that no security assessment had been performed on the supposedly isolated CES network. (See Exhibit D, p. 4.)

44.

While KSU UITS Information Security Office was attempting to correct the multiple security failures at CES, King was, on information and belief, bringing its backup server online. (See email chain from Michael Barnes, Director CES, to King, dated March 4, 2017, attached as “Exhibit E.”) On March 3, 2017, King brought the CES backup server online, and, on March 4, 2017, KSU UITS Information Security Office discovered that, in doing so, King had again exposed confidential information. (See id.)

45.

The backup server hosted election databases and programs similar to those Lamb and Grayson had accessed, all available without authentication or authorization to people on the campus network. (See Exhibit E, pp. 2 – 3.)

46.

On March 4, 2017, shortly after discovering that the backup server was on line, KSU UTIS requested that the server be shut down until further assessment could be made and sensitive data protected. The server was reportedly shut down approximately one and a half hours later, at about 7:00 pm. (See Exhibit E.)

47.

This at least seven-month long security breach constituted just one example of the irregularities and misconduct preceding and associated with the Runoff, as

detailed below. Further, even if the security breaches resulted in no detectable manipulation of the Runoff election process, the DRE system employed did not and can never meet Georgia’s statutory requirements. Nevertheless, on June 20, 2017, the Runoff was held to fill a vacancy left by the previous incumbent, Congressman Tom Price, and was conducted as if such security failures had not occurred. On the evening of June 26, 2017, within minutes of the certification of the result from DeKalb County, the final county to certify the result, Secretary Kemp, fully aware of the security failures, certified Handel as the winner of the election.⁶ As noted below, the Runoff and certification of Handel were undertaken in violation of Plaintiffs’ constitutional and statutorily protected rights.

B. Defendants Violated Plaintiffs’ Right To Vote in the Runoff on Systems That Would Correctly Count Their Votes.

48.

The right to vote is the foundation of our democracy. It is how we ensure that our government has the consent of the governed. It is enshrined in the

⁶ Kemp Certifies June 20 Runoff, Office of the Secretary of State of the State of Georgia, June 27, 2017, http://sos.ga.gov/index.php/general/kemp_certifies_june_20_runoff (last visited July 3, 2017).

O.C.G.A. § 21-2-524 requires that “A petition to contest the result of a primary or election shall be [...] within five days after the official consolidation of the returns of that particular office or question and certification thereof by the election official having responsibility for taking such action under this chapter.” This would place the filing deadline on Saturday July 1, 2017. O.C.G.A. § 1-3-1(d)(3) (“When the period of time prescribed is less than seven days, intermediate Saturdays, Sundays, and legal holidays shall be excluded in the computation.”) Thus, the deadline for filing a challenge to the Runoff was July 3, 2017.

Constitution of the United States and in the Constitution of the State of Georgia.

Electors have the right to vote, the right to do so by a legally constructed ballot, the right to have their ballots accurately tabulated, and the right to be assured that their votes will be counted and recorded accurately and in compliance with Georgia law.

When electors have a factual basis not to trust that their votes will be accurately counted and recorded, it has a chilling effect and violates those rights. When, as in the Runoff, votes are not properly recorded or counted—or cannot be independently audited and verified, with discrepancies corrected—then those rights have been violated. In fact, the Georgia Constitution at Article II, Section I, provides an unusual measure of protection for the purity of elections and Georgia electors' rights by incorporating the requirement for election officials to comply with all election statutes in the State Constitution.

49.

Plaintiffs are electors who are residents of Georgia, including residents of Georgia's 6th Congressional District, as well as an association that includes among its members electors of the State of Georgia, who are concerned about the integrity, credibility, security, and reliability of the electoral process.

50.

Georgia's 6th Congressional District spans portions of Fulton, Cobb, and DeKalb counties.

51.

Defendants Secretary Kemp, Members of the State Election Board, and the State Board (“Statewide Election Officials”) used, and instructed the use of, Georgia’s DRE System and Optical Scanning System to conduct the Special Election and Runoff in Georgia’s 6th District.

52.

Defendants Barron, Members of Fulton County Board of Registration and Elections, and the Fulton Board (“Fulton County Election Officials”) used Georgia’s DRE System and Optical Scanning System to conduct the Special Election and Runoff in Fulton County.

53.

Defendants Daniels, Members of DeKalb County Board of Registration and Elections, and the DeKalb Board (“DeKalb County Election Officials”) used Georgia’s DRE System and Optical Scanning System to conduct the Special Election and Runoff in DeKalb County.

54.

Defendants Eveler, Members of Cobb County Board of Elections and Registration, and the Cobb Board (“Cobb County Election Officials”)⁷ used

⁷ The Fulton County Election Officials, DeKalb County Election Officials, and Cobb County Election Officials are collectively referred to as “County Election Officials.”

Georgia’s DRE System and Optical Scanning System to conduct the Special Election and Runoff in Cobb County.

1. Georgia’s Voting System Has Fundamental Flaws.

55.

To conduct its elections, Georgia employs more than one “system,” as that term is defined by statute. Thus, as used herein, “Georgia’s Voting System” refers to the totality of the physical, electronic, and legal infrastructure related to the processes and procedures of voting, counting votes, and conducting elections in general. Georgia’s Voting System is primarily comprised of a “DRE System,” governed by Georgia Code Sections 21-2-379.1 to -379.12, and an “Optical Scanning System” governed by Georgia Code Sections 21-2-365 to -379. Georgia’s DRE System did not and can never meet Georgia’s statutory requirements. On the other hand, the Optical Scanning System, although non-compliant in the Runoff because of security breaches, can be brought into compliance with Georgia law in future elections.

56.

For in-person voting, including election day voting, Georgia primarily uses voting computers, referred to as DRE voting machines, along with various voting and tabulation programs, that, when working properly, directly record an elector’s vote on an electronic medium (“DRE System”). See O.C.G.A. §§ 21-2-379.1 to -

379.12; see also Ga. Comp. R. & Regs. 183-1-12.01. The DRE voting machines used in Georgia, unlike other voting methods, do not allow voters to verify that their votes have been correctly recorded and do not create auditable paper records of votes cast. (See Affidavit of Edward W. Felten ¶¶ 5 – 6, attached as “Exhibit F.”) This absence of a paper trail is the reason “computer scientists and cybersecurity experts typically recommend against the use of DREs.” (Id., ¶7.)

57.

On information and belief, Georgia’s DRE System, currently in use in all 159 of Georgia’s counties in various configurations, consists of the following components and related firmware and software:

- Touch Screen: R6 – Ballot Station 4.5.2! and TSx – Ballot Station 4.5.2!;
- ExpressPoll: ExpressPoll 4000 and 5000 running software; EZRoster; 2.1.2 and Security Key 4.5+ with Card Writer 1.1.4;
- Election Management System: GEMS 1.18.22G!; and
- Honeywell barcode scanner: MK1690-38-12-ISI, used with ExpressPoll pollbooks.

This configuration, referenced herein as the “DRE System,” was used to accept and process the majority of votes in the Runoff despite the fact that its use does not comply with Georgia statutes for DRE systems provided for in Georgia Code Section 21-2-379.

58.

Georgia Code Section 21-2-379.2(c) prohibits the use, in any primary or election, of any kind of DRE voting system that the Secretary of State has not certified can be “safely or accurately used.” The intent of this rule is to ensure that “hardware, firmware, and software have been shown to be reliable, accurate, and capable of secure operation before they are used in elections in the state.” Ga. Comp. R. & Regs. 590-8-1-.01(a)(3). On information and belief, the Secretary of State never approved of or certified the DRE System as safe and accurate in its current form, nor is it possible that he can do so in the future because the DRE System cannot be brought into compliance with the provisions of Section 21-2-379.

59.

For absentee ballots, Georgia primarily uses Optical Scanning voting machines, along with various tabulation and report generation programs (“Optical Scanning System”). See O.C.G.A. §§ 21-2-365 to -379; see also Ga. Comp. R. & Regs. 183-1-12.01.

60.

On information and belief, Georgia’s Optical Scanning System, as currently used in Georgia’s elections consists of the following configuration of components and related firmware and software:

- Optical Scanner: AccuVote OS 1.94W and
- Election Management System: GEMS 1.18.22G!

61.

Georgia Code Section 21-2-368(c) prohibits the use, in any primary or election, of any kind of Optical Scanning System that the Secretary of State has not certified can be “safely or accurately used.” The intent of this rule is to ensure that “hardware, firmware, and software have been shown to be reliable, accurate, and capable of secure operation before they are used in elections in the state.” Ga. Comp. R. & Regs. 590-8-1-.01(a)(3). On information and belief, the Secretary of State never approved of or certified the Optical Scanning System as safe and accurate in its current form and as was used in the Runoff.

62.

County Election Officials likewise had a duty to certify the equipment used in the Optical Scanning System. Georgia Code Section 21-2-368(d) states that, “[a]t least ten days prior to any primary or election, including special primaries, special elections, and referendum elections, the election superintendent shall verify and certify in writing to the Secretary of State that all voting will occur on equipment certified by the Secretary of State.” On information and belief, County Election Officials did not do so for the Runoff. By so failing, the County Election

Officials violated the Election Code and the rights of the electors in their respective counties.

63.

Georgia's DRE System and Optical Scanning System are fifteen years old, run on an insecure operating system that is years past its support life, and rely on the same tabulation software and server, GEMS, that was exposed by the security failures at CES.

64.

Security researchers have repeatedly demonstrated that the hardware and software of the types used by Georgia are vulnerable to hacking. (See Exhibit F.) For example, in 2006, security researchers from Princeton, including Edward W. Felten, the former Deputy U.S. Chief Technology Officer, were able to hack an AccuVote TS, the primary DRE machine in use in Georgia, in less than four minutes using just \$12 worth of tools.⁸ This hack allowed them to infect a single AccuVote TS machine in a way that would spread to the total election result when the device's memory card was used to tabulate the result.⁹ The researchers were

⁸ Daniel Turner, How to Hack an Election in One Minute, MIT Technology Review, September 18, 2016, <https://www.technologyreview.com/s/406525/how-to-hack-an-election-in-one-minute/> (last visited June 30, 2017).

⁹ Id.

able to prove that these machines could be physically hacked in a matter of minutes, that malicious software could be installed, and that malicious software could then spread.¹⁰ (See also Exhibit F.) Since these machines do not provide a voter-verified paper ballot, there is no independent method to confirm that votes were counted, and counted as cast.

65.

Because of accuracy concerns, several states have decertified these voting machines and/or the software running on them. For example, in 2006 Maryland's House of Delegates voted unanimously to stop using these machines,¹¹ North Carolina has banned the use of DRE machines that do not produce voter-verifiable paper ballots, like those used in Georgia's DRE System, beginning in 2018,¹² and in 2009 the Secretary of State for the State of California decertified the code running on them, GEMS 1.18.19.¹³ The version of GEMS that California decertified was only three minor revisions earlier than the version of GEMS now

¹⁰ Id.

¹¹ Common Sense in Maryland, New York Times, March 23, 2006, <http://www.nytimes.com/2006/03/23/opinion/common-sense-in-maryland.html?mcubz=1> (last visited June 30, 2017).

¹² See N.C. Gen. Stat. §§ 163-165.1. to -165.10.

¹³ Withdrawal of Approval of Premier Election Solutions, Inc./Diebold Election Systems, Inc., GEMS 1.18.19, Office of the Secretary of State of the State of California, March 30, 2009, <http://votingsystems.cdn.sos.ca.gov/vendors/premier/premier-11819-withdrawal-approval033009.pdf> (last visited June 30, 2017).

being used in Georgia in both its DRE System and its Optical Scanning System, GEMS 1.18.22.G!.

66.

These problems are exacerbated by the fact that Georgia uses DRE machines (voting computers) that run on antiquated software that is programmed by and downloaded from one central location: CES. (Exhibit F, ¶26.) This makes Georgia far easier to infiltrate than states that use multiple systems that are distributed and managed at the county level across the state, as only one vulnerable site in Georgia (CES) needs to be exploited to manipulate the entire state's elections. On information and belief, due to press reports of Lamb's and Grayson's access of CES as well as an earlier lawsuit, these security vulnerabilities were known to Defendants.

67.

The fact that the electronic infrastructure, including all election management data and programs, is centralized at a single location, CES, provides a tempting and vulnerable target. Since CES exposed passwords to the server, exposed code, left key rooms unlocked, and permitted unauthorized internet access, the election tabulation programming and election data were left open to manipulation by malicious hackers. (See Exhibits A and D.) Such security failures would impact both the DRE System and the Optical Scanning System, since both use the same

tabulation program. In other states, a single point of failure would not render the entire state's election suspect as most use decentralized systems.

68.

Furthermore, would-be hackers can gain physical access to the hardware, firmware, and software with relative ease, given lax storage policies. On information and belief, the physical security of DRE voting equipment used in Georgia's DRE System has been inadequate during pre- and post-election machine storage, leaving the machines vulnerable to attack and compromise. During the Runoff (and in past elections), the security practices and procedures did not comply with the statutory requirements for storage of DRE units.

As Dr. Felten notes:

Because of the vulnerability of the DRE voting machines to software manipulation, and because of the intelligence reports about highly skilled cyber-attackers having attempted to affect elections in the United States, [stringent] precautions appear to be indicated for the CES systems. In the absence of stringent precautions to find and expel potential intruders in the CES systems, the ability of voting-related systems that have been in the CES facility to function correctly and securely should be viewed with greater skepticism. (Exhibit F, ¶ 29.)

69.

A further vulnerability of Georgia's Voting System derives from the fact that, on information and belief, on all election nights, Fulton County transmits ballot data from touchscreen machine memory cards to the GEMS tabulation

server via a modem in an unauthorized configuration that does not use adequate encryption. Applicable voting system standards require that security of data transmission be assured. The lack of security in electronic transmission exposes both the memory cards and the GEMS system to, and invites, attack.

70.

On information and belief, the physical security of DRE voting equipment used in Georgia's DRE System has been inadequate during pre- and post-election machine storage, in violation of Georgia Code Section 21-2-379.9 and the rules and regulations promulgated thereunder. See Ga. Comp. R. & Regs. 183-1-12.02(2). These security failures have left and continue to leave the machines, and thus the entire DRE System, vulnerable to attack and compromise.

71.

On information and belief, Georgia's Voting System does not meet minimum standards, including mandatory audit capacity standards, required by the Help America Vote Act, 52 U.S.C. § 21081.

72.

There are additional significant security and accuracy violations that prevented Georgia's Voting System, including the DRE System and the Optical Scanning System, from being used safely and accurately in the Runoff. Such violations and non-compliance prevent the certification and use of Georgia's DRE

System. (See Exhibits A; D; F; Affidavit of Duncan Buell, attached as “Exhibit G”; Declaration of Barbara Simons, attached as “Exhibit H.”)

2. Defendants Failed to Heed Warnings of Outside Threats to Georgia’s Voting System.

73.

According to then-Director of the Federal Bureau of Investigation (“FBI”), James Comey, hackers were “scanning” election systems in the lead-up to the election in the fall of 2016.¹⁴ Subsequent reporting has suggested that as many as 39 states were targeted.¹⁵ Secretary Kemp, through his spokesman, has denied that Georgia was one of the states so targeted.¹⁶

¹⁴ Kristina Torres, Georgia Not One of 20 States Targeted by Hackers Over Election Systems, Atlanta Journal-Constitution, September 30, 2016, (<http://www.ajc.com/news/state--regional-govt--politics/georgia-not-one-states-targeted-hackers-over-election-systems/FvCGGjulVUm7VNMp8a9vuO/>) (last visited June 30, 2017).

¹⁵ Michael Riley and Jordan Robertson, Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known, BloombergPolitics, June 13, 2017, <https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections> (Last visited June 30, 2017).

¹⁶ Kristina Torres, State Considers Dropping Election Data Center, Atlanta Journal-Constitution, June 14, 2017, <http://www.myajc.com/news/state--regional-govt--politics/state-considers-dropping-election-data-center/YLERatmHYmLEqnOjUng2GL/> (last visited June 30, 2017).

74.

In August 2016 the Department of Homeland Security (“DHS”) offered assistance to any state that wanted help securing its electronic election infrastructure.¹⁷ Secretary Kemp refused the offer.¹⁸

75.

Around the same time, on August 23, 2016, the Election Assistance Commission (“EAC”) sent to various state election officials, including Secretary Kemp, an email sharing an alert from the FBI. (See Exhibit B.) This email attached a copy of the FBI’s August 18, 2016 alert number T-LD10004-TT, which provided detailed information on the cybersecurity threats facing the nation’s election systems and recommended specific steps that should be taken to reduce the risk. (See id.)

76.

Despite the warnings from DHS, the FBI, and the EAC, on information and belief, no entity or responsible official, including Secretary Kemp, King, or any election official, took meaningful action to ensure the security of Georgia’s Voting

¹⁷ DHS Press Office, Readout of Secretary Johnson’s Call With State Election Officials on Cybersecurity, Department of Homeland Security, August 15, 2016, <https://www.dhs.gov/news/2016/08/15/readout-secretary-johnsons-call-state-election-officials-cybersecurity> (last visited June 30, 2017).

¹⁸ Marshall Cohen and Tom LoBianco, Hacking the Election? Feds Step in as States Fret Cyber Threats, CNN, September 23, 2016, <http://www.cnn.com/2016/09/23/politics/ohio-pennsylvania-election-2016-hack/index.html>, (last visited June 30, 2017).

System or acted to bring it into compliance with Georgia’s statutes and regulations. Press reports indicate that Georgia was the only state to refuse all federal assistance to help ensure the security of its election infrastructure.¹⁹

77.

After the CES security breach had been reported, Defendants received more warnings of the need to secure Georgia’s Voting System. For example, on March 15, 2017, a group of over 20 experts in the field of computer security and voting systems sent a letter to Secretary Kemp expressing their concerns with the security of Georgia’s election systems. (See letter from various experts to Secretary Kemp dated March 15, 2017, attached as “Exhibit I,” pp. 1-2.) And on March 16, 2017, the Democratic Party of Georgia, also responding to those reports, wrote Kennesaw State University, copying Secretary Kemp, expressing concerns over the security of the election.²⁰

¹⁹ Massimo Calabresi, Inside the Secret Plan to Stop Vladimir Putin’s U.S. Election Plot, Time, July 20, 2017, <http://time.com/4865982/secret-plan-stop-vladimir-putin-election-plot/> (last visited July 27, 2017).

²⁰ Letter from Chairman DuBose Porter, Democratic Party of Georgia to President Samuel S.Olens, Kennesaw State University, March 16, 2017, <http://www.georgiademocrat.org/wp-content/uploads/2017/03/KSU-Letter-of-Request-031617.pdf> (last visited June 30, 2017).

78.

As with the warnings from DHS, the FBI, and EAC, none of these warnings appear to have resulted in any meaningful remedial action on the part of any of the Defendants, demonstrating their misconduct and abuse of discretion.

3. Stolen Electronic Pollbooks Escalated Risk of Compromised Election.

79.

On April 15, 2017, an additional known security breach occurred when four electronic pollbooks containing a voter registration database and software to program voter access cards were stolen from an election worker's truck.²¹ The Chairman of the Cobb County GOP was quoted as saying that, "The theft could just be a random thing, but the timing makes it much more worrisome, [...] I think there is cause to be concerned about the integrity of the elections."²² Pollbooks are used to confirm a voter's name and address and to create a voter access card for the DRE machine. Once chain of custody of a pollbook is lost, officials must presume that black market copies exist and will be used for illicit purposes.

²¹ Christopher Wallace, New details emerge in theft of Ga. Voting machines, Fox News April 18, 2017, <http://www.foxnews.com/politics/2017/04/18/new-details-emerge-in-theft-ga-voting-machines.html>, (last visited June 30, 2017).

²² Id.

80.

On information and belief, this theft of electronic pollbooks did not motivate Secretary Kemp and other Defendants to take adequate remedial action.

4. Special Election Irregularities Were Recklessly Minimized.

81.

Technical problems arose during the April 18th Special Election. For example, Fulton County voters were being improperly sent from one precinct to another to vote due to glitches in the electronic pollbook software. In addition, the Special Election experienced technical problems caused by Fulton County's uploading of improper and unauthorized memory cards—something the system is not supposed to allow—resulting in errors and delays in uploading election results.²³

82.

On information and belief, unconventional procedures, including deleting precinct voting results in the database, were used to attempt to correct the error caused by Fulton County's uploading of improper and unauthorized memory cards, but the purported corrections themselves lacked a verifiable audit trail.

²³ Arielle Kass, 'Rare Error' Delays Fulton County Vote Counts in 6th District Race, Atlanta Journal-Constitution, April 19, 2017, <http://www.ajc.com/news/local-govt--politics/rare-error-delays-fulton-county-vote-counts-6th-district-race/dleYXJvjL1R9gSsw1swwAJ/> (last visited June 30, 2017).

83.

On May 24, 2017, after becoming aware of the database breach, pollbook theft, and problems with the electronic tabulation of the votes cast in Fulton County in the Special Election, sixteen computer scientists wrote Secretary Kemp to express profound concerns about the lack of verifiability and unacceptable security of Georgia's Voting System. (See Letter from various experts to Secretary Kemp dated May 24, 2017, attached as "Exhibit J.") The computer scientists urged Secretary Kemp to treat the breach at CES "as a national security issue with all seriousness and intensity." (*Id.*, p 1.) They stated that "a truly comprehensive, thorough and meaningful forensic computer security investigation likely would not be completed in just a few weeks." (*Id.*) They warned that the error that occurred in Fulton County during the Special Election could indicate a corrupted database that must be investigated, and urged the use of paper ballots. (*Id.*, p. 2.)

84.

These errors were sufficiently severe that Secretary Kemp called for an investigation into them.²⁴ No results from this investigation have been announced, nor has the public been told that it has been completed. Yet with that pending investigation ongoing and warnings from credible sources, Defendants improperly

²⁴ Aaron Diamant and Berndt Petersen, State Opens Investigation into Issues With 6th District Race, WSBTV, May 26, 2017, <http://www.wsbtv.com/news/local/atlanta/state-opens-investigation-into-issues-with-6th-district-race/514213222> (last accessed June 30, 2017).

instructed that the Runoff be conducted on the compromised voting systems, which constitutes official misconduct, abuse of discretion, and election irregularity.

5. Defendants Were Authorized to Use Only Certified Elections Systems That Would Ensure Plaintiffs' Votes Were Properly Counted.

85.

Prior to the Runoff, Kemp and King were aware of the multiple security breaches at CES, the unresolved theft of the electronic pollbooks, pollbook problems in the Special Election, Fulton County memory card issues, the non-compliance with Georgia election statutes, and the security issues raised in Curling v Kemp (Case No. 2017CV290630).

86.

Georgia law explicitly allows the Secretary of State to, “at any time, in his or her discretion,” reexamine the voting systems used in Georgia, and to prevent their use if they “can no longer be safely or accurately used.” O.C.G.A. § 21-2-368; O.C.G.A. § 21-2-379.2. Despite this, Secretary Kemp allowed the Special Election and Runoff to be run on compromised systems with the knowledge that they could not be presumed to be able to be “safely or accurately used by electors.” Id.

87.

Georgia Code Section 21-2-379.2(a) grants to any ten or more concerned electors the right to require the Secretary of State “at any time” to conduct a

reexamination of a previously examined and approved DRE voting system.

Specifically, Section 21-2-379.2(a) reads as follows:

(a) Any person or organization owning, manufacturing, or selling, or being interested in the manufacture or sale of, any direct recording electronic voting system may request the Secretary of State to examine the system. Any ten or more electors of this state may, at any time, request the Secretary of State to reexamine any such system previously examined and approved by him or her. Before any such examination or reexamination, the person, persons, or organization requesting such examination or reexamination shall pay to the Secretary of State the reasonable expenses of such examination. The Secretary of State may, at any time, in his or her discretion, reexamine any such system.

Id. The clear intent of the statute is to permit a timely reexamination of a voting system in question prior to a pending election.

88.

Georgia Code Section 21-2-379.2(b) provides that, upon receiving such a request for reexamination from ten or more electors, the Secretary of State has a duty to reexamine the DRE voting system. The statute reads as follows:

(b) The Secretary of State shall thereupon examine or reexamine such direct recording electronic voting system and shall make and file in his or her office a report, attested by his or her signature and the seal of his or her office, stating whether, in his or her opinion, the kind of system so examined can be safely and accurately used by electors at primaries and elections as provided in this chapter. If this report states that the system can be so used, the system shall be deemed approved; and systems of its kind may be adopted for use at primaries and elections as provided in this chapter.

Id.

89.

Importantly, Section 21-2-379.2(c) makes clear that if a DRE voting system has not been certified by the Secretary of State, then it may not be “used at any primary or election.” O.C.G.A. § 21-2-379.2(c) provides that:

(c) No kind of direct recording electronic voting system not so approved shall be used at any primary or election and if, upon the reexamination of any such system previously approved, it shall appear that the system so reexamined can no longer be safely or accurately used by electors at primaries or elections as provided in this chapter because of any problem concerning its ability to accurately record or tabulate votes, the approval of the same shall immediately be revoked by the Secretary of State; and no such system shall thereafter be purchased for use or be used in this state.

Id. (emphasis added).

90.

Likewise, Georgia Code Section 21-2-368(a) authorizes the Secretary of State “at any time” to conduct a reexamination of a previously examined and approved optical scanning voting system. Specifically, Section 21-2-368(a) reads as follows:

(a) Any person or organization owning, manufacturing, or selling, or being interested in the manufacture or sale of, any optical scanning voting system may request the Secretary of State to examine the optical scanning voting system. Any ten or more electors of this state may, at any time, request the Secretary of State to reexamine any optical scanning voting system previously examined and approved by him or her. Before any

such examination or reexamination, the person, persons, or organization requesting such examination or reexamination shall pay to the Secretary of State the reasonable expenses of such examination. The Secretary of State may, at any time, in his or her discretion, reexamine any optical scanning voting system.

Id. The clear intent of the statute is to permit a timely reexamination of a voting system in question prior to a pending election.

91.

Georgia Code Section 21-2-368(b) provides that, upon determining that a reexamination is needed, the Secretary of State has a duty to reexamine the optical scanning voting system. The statute reads as follows:

(b) The Secretary of State shall thereupon examine or reexamine such optical scanning voting system and shall make and file in his or her office a report, attested by his or her signature and the seal of his or her office, stating whether, in his or her opinion, the kind of optical scanning voting system so examined can be safely and accurately used by electors at primaries and elections as provided in this chapter. If this report states that the optical scanning voting system can be so used, the optical scanning voting system shall be deemed approved; and optical scanning voting systems of its kind may be adopted for use at primaries and elections as provided in this chapter.

Id.

92.

Section 21-2-368(c) provides that, if reexamination shows that an optical scanning voting system “can no longer be safely or accurately used,” then the approval of that system “shall immediately be revoked by the Secretary of State;

and no such system shall thereafter ... be used in this state.” (emphasis added). The statute reads as follows:

(c) No kind of optical scanning voting system not so approved shall be used at any primary or election and if, upon the reexamination of any such system previously approved, it shall appear that the optical scanning voting system so reexamined can no longer be safely or accurately used by electors at primaries or elections as provided in this chapter because of any problem concerning its ability to accurately record or tabulate votes, the approval of the same shall immediately be revoked by the Secretary of State; and no such system shall thereafter be purchased for use or be used in this state.

Id. Importantly, Section 21-2-368(c) makes clear that if an optical scanning voting system has not been certified as safe and accurate by the Secretary of State, then it may not be “used at any primary or election.”

93.

On information and belief, Georgia began using a DRE System to conduct its elections in 2002. The devices used were certified for use by the then Secretary of State, Cathy Cox (“Secretary Cox”). (Certification of Election Systems for use in Georgia, attached as “Exhibit K.”) Secretary Cox again certified these systems in 2003, 2004, 2005, and 2006. (Id.) Her successor, Karen Handel, certified the DRE System that was used in 2007 and 2008.²⁵ (Id.) On information and belief, this is the last time a Georgia Secretary of State certified a DRE voting system for

²⁵ Although the certification was expressly for the DRE System, certain optical scanning components were included in the certifications from 2004 to 2008.

use in Georgia—and even then, it was without explicitly opining on the safety and accuracy of the system, as is further required by § 21-2-379.2(b).

94.

On information and belief, Secretary Kemp has never—in the past seven years of his two terms in office as Secretary of State—certified that Georgia’s DRE System “can be safely and accurately used by electors at primaries and elections,” as required by Georgia law. O.C.G.A. § 21-2-379.2(b). The most recently certified system has been subject to material modifications since its certification in 2008—almost ten years ago. Kemp himself penned a 2015 op-ed stating that, “Each time a component is changed, the entire system is retested to ensure there are no unintended consequences.”²⁶ Yet, Kemp and King negligently avoided undertaking such testing and re-certification in advance of the Special Election and Runoff even after being requested to do so by electors.

95.

On information and belief, Secretary Kemp has also never certified that Georgia’s Optical Scanning System “can be safely and accurately used by electors at primaries and elections,” as required by Georgia law. O.C.G.A. § 21-2-368(b).

²⁶ Brian Kemp, *Georgia’s Voting System in Great Shape*, Atlanta Journal-Constitution, October 29, 2015, <http://www.myajc.com/news/opinion/georgia-voting-system-great-shape/T49mQ6KNioWWLUJUYQg68L/> (last visited August 2, 2017).

96.

Given the known vulnerabilities in the system, the security breaches, and—most importantly—the DRE System’s inability to meet statutory requirements (as detailed in Section IV.E.), Secretary Kemp would have been unable to make a good faith determination that the DRE System or the Optical Scanning System could be “safely and accurately used.” O.C.G.A. § 21-2-379.2(b); O.C.G.A. § 21-2-368(b).

97.

On May 10, 2017, based on the publicly available information, and fearing that the Runoff could be compromised, a group of Georgia electors, including Davis, exercised their rights under O.C.G.A. § 21-2-379.2(a) by requesting that Georgia’s Voting System be reexamined and listing a number of security concerns. On May 17, 2017, a second letter was sent explaining the irreversible security issues in the system in support of the request that Georgia’s Voting System be immediately reexamined. Two additional letters followed, on May 19 and June 2, each requesting a timely response. No answer was received until after the electors filed suit on May 25, 2017 against Secretary Kemp over his failure to reexamine the system. See Curling v. Kemp, Case No. 2017CV290630.

97.

The Secretary of State's Office did not respond to the electors' requests until June 5, 2017. It indicated that it would complete the reexamination in approximately six months, putting the completion date after the date of elections that will be held in November. (See letter from C. Ryan Germany to various electors dated June 5, 2017, attached as "Exhibit L.")

98.

Pending the reexamination, Secretary Kemp declined to use his authority under Georgia Code Section 21-2-379.2 to prevent the use of the unsecure DRE System for the Runoff and declined to use his authority under Section 21-2-368 to prevent the use of the Optical Scanning System for the Runoff—despite the fact that Georgia law allows for voting to be done by paper ballot if the voting system is unusable.

99.

Georgia's election laws contemplate that elections normally required to be conducted using voting equipment may instead be conducted using paper ballots if circumstances so require. O.C.G.A. § 21-2-281. The County Election Officials maintain the authority and responsibility for making the decision to employ paper ballots when "the use of voting equipment is impossible or impracticable." O.C.G.A. § 21-2-334. Moreover, Georgia Code Section 21-2, Article 11, Part 2,

provides the detailed procedures that are required to be used in precincts that conduct primaries and elections using paper ballots. County Election Officials abused their discretion by failing to exercise this authority to order the use of paper ballots.

C. Improper Certification of the Election Results

100.

To provide for election transparency and citizen oversight of Georgia elections, Georgia election regulations provide for citizen-initiated recanvassing of any precincts that seem to have erroneous results from the DRE-voting machines. Ga. Comp. R. & Regs. 183-1-12.02(7). These regulations permit citizens to choose any or all precincts to demand recanvassing of the votes, by having the memory cards reread by the tabulation server and conducted by the election officials prior to the county-level certification of results.

101.

Members of CGG (then Rocky Mountain Foundation) and other citizens wrote to DeKalb Board and Cobb Board prior to county-level certification, specifying the precincts they believed may contain erroneous results and requesting a recanvassing prior to the certification. (See letters to DeKalb Board and Cobb Board by various electors, attached as “Exhibit M.”) On information and belief, and in each case, a board discussion was held and Defendants Barron,

Daniels, Cobb Board, DeKalb Board, Members of Cobb County Board of Elections and Registration, and Members of DeKalb County Board of Registration and Elections affirmatively denied the electors' properly submitted requests for recanvassing, constituting an irregularity and misconduct on the part of these Defendants.

102.

Prior to each county election board meeting, on behalf of its members who are eligible electors in the 6th Congressional District, CGG filed letters requesting that Fulton Board, Cobb Board, and DeKalb Board (collectively "County Boards") deny certification of the election because of the numerous violations of law occurring during the conduct of the election. (See letters to County Boards by CGG (then Rocky Mountain Foundation), attached as "Exhibit N.") On information and belief, these letters (and the concerns expressed) were not discussed at any of the County Boards. Instead, the County Boards simply rubberstamped the results without concern about the legality or accuracy of the returns or violations of the Election Code in the conduct of the Runoff. The County Boards' and their individual members' and Directors' refusal to consider the alleged illegal aspects of the election constitute irregularities, misconduct and abuse of discretion.

103.

On information and belief, Secretary Kemp almost immediately certified the consolidated return for the Runoff after the last certification, the DeKalb Board certification, had taken place, despite the fact that he had been informed that the County Boards had violated electors' rights to seek a recanvass of precincts that appeared to show irregularities or questionable results. Certification of the consolidated return with valid pending requests for recanvass and known system security failures constitutes an irregularity and misconduct on the part of Secretary Kemp.

D. Irreparable Harm/Inadequate Remedy at Law

104.

Georgia electors who cast their votes in person during the Runoff were required to cast their votes on voting computers using the DRE System in early voting locations or on June 20, 2017 in their neighborhood precincts.

105.

Georgia electors who cast their votes by absentee ballot during the Runoff were required to cast their votes using the Optical Scanning System.

106.

Georgia's DRE System could not be safely and accurately used by electors voting in the Runoff. Georgia's DRE System violates numerous provisions of the

Election Code, is demonstrably vulnerable to undetectable malfunctions and malicious manipulation that cannot be corrected on a timely or reasonable basis, and results in electors' casting ballots that cannot be independently audited or verified.

107.

Georgia's Optical Scanning System could not be safely and accurately used by electors voting in the Runoff. Georgia's Optical Scanning System, as configured for the Runoff, violated numerous provisions of the Election Code and was demonstrably vulnerable to undetectable malfunctions and malicious manipulation that could not be detected or corrected on a timely or reasonable basis.

108.

Each Plaintiff who cast a vote in the Runoff and the Georgia 6th Congressional District elector members of Plaintiff CGG were harmed in the exercise of their constitutional fundamental right to vote in the Runoff because Georgia used an illegal, unsafe, unsecure, and uncertified DRE System and Optical Scanning System that were subjected to undetected, unauthorized access and potential manipulation. Experts concur in the conclusion that the systems and their components had to be considered compromised and unreliable for the determination of the result. (See Exhibits A, F, G, and H.)

E. Georgia's DRE System Violates the Election Code.

109.

Election officials, including all Defendants, are responsible for willful, substantive violations of the Election Code, causing the votes cast by the majority of voters to be cast as illegal ballots on the unauthorized, non-compliant DRE System.

110.

All Defendants conducted the election by employing procedures that violate mandatory and essential security provisions of the Election Code. Such violations include but are not limited to the following:

111.

First, the DRE voting machines were not evaluated and cannot be evaluated to determine whether they meet the requirement of Georgia Code Section 21-2-379.1(8): "It shall, when properly operated, record correctly and accurately every vote cast."

112.

Second, the superintendents did not and cannot meet the requirement of Georgia Code Section 21-2-379.6(a) to determine that the DRE machines have no votes recorded at the opening of the polls. The State's testing methods cannot

determine whether there are votes recorded on the machine before voting is authorized.

113.

Third, superintendents failed to meet basic, reasonable security of machines in the polling place prior to and after the operation of the polls, as mandated by Georgia Code Section 21-2-379.6(a) in a manner to prevent the operation of the “counting machinery” before such operation is authorized. Machines used in the Runoff have been frequently left unattended in public hallways, as they were during the Runoff, with inadequate physical locks and seals, subjecting the “counting machinery” to undetectable manipulation. Id.

114.

Fourth, the State Board and Secretary Kemp have failed to perform their duty to promulgate adequate security regulations to protect the DRE machines from intrusion and manipulation pursuant to Georgia Code Section 21-2-379.6(a).

115.

Fifth, the DRE machines (voting computers) do not and cannot meet the mandatory testing standard provisions of Georgia Code Section 21-2-379.6(c), which require that the machines be tested to determine whether they count votes accurately. Testing conducted by the state’s Logic and Accuracy Testing did not

and cannot determine whether the machines correctly count the votes in the Runoff.

116.

Sixth, the DRE machines did not and cannot meet the mandatory provisions of Georgia Code Section 21-2-379.7(b) requiring that machines be “thoroughly tested” and certified as to their ability to work properly and to ensure that no votes are recorded in the machine before the opening of the polls. Officials did not and cannot verify whether the DRE machines are “working properly.” Id.

117.

Seventh, in violation of Georgia Code Section 21-2-379.7(c), the superintendents and poll managers failed to provide adequate protection against “molestation and injury” to the machines when they were stored at polling places. The State Board and Secretary Kemp failed to provide adequate rules to assure reasonable security of the equipment, causing the equipment to be stored in public places with minimal and ineffective security. Under such circumstances, the machines must be presumed to have been compromised, generating an unreliable result.

118.

Eighth, the tabulation mechanisms on the DRE machines were not secured by the poll managers during the machines’ use on election day as mandated by

Georgia Code Section 21-2-379.7(d)(3). Such security requirements became impossible to meet after the CES system was open to the internet as described in ¶¶ 26 – 47.

119.

Ninth, the DRE units have not been maintained in secure storage when not in use as required by Georgia Code Section 21-2-379.9(b), nor have the DRE machines been stored in compliance with Ga. Comp. R. & Regs 183-1-12-.02(2)(b). As a result, the machines have been subjected to significant unknown risks, leaving no practical way to evaluate whether the machines were compromised.

120.

Tenth, Georgia Code Section 21-2-379.9(b) requires that the DRE “related equipment” for the operation of the election (such as the GEMS servers, memory cards, and electronic pollbooks) be secured. However, conditions at CES, as well as in each County Election Official’s location, were such that the “related equipment” was not properly secured, which exposed the components and voting system to significant risk. (See Exhibit D.) It was impossible for County Election Officials to determine the impact of this long-term exposure to significant risk and whether the system was compromised to operate improperly.

121.

Eleventh, any new voting system deployed after April 17, 2005 is required to meet the certification standards in Ga. Comp. R. & Regs. 590-8-1-.01. That regulation requires compliance with the most recent EAC voting standards for certification of a new voting system or substantive change in a previously certified system. On information and belief, Secretary Kemp has not attempted to certify the DRE System to those mandatory state standards, nor has he certified that it meets those standards although the current equipment configuration constitutes a new system deployed after April 17, 2005. In fact, because inherent weaknesses render it incapable of meeting statutory requirements, the DRE System cannot be legally certified, approved, or utilized. It is impossible for the DRE System to meet the requirements of the Election Code. Yet, on information and belief, Secretary Kemp and King have knowingly made misleading public claims that the voting system was “federally and state certified.”

F. Georgia’s Optical Scanning System Violates the Election Code.

122.

All Defendants are responsible for willful substantive violations of the Election Code, causing the votes cast by the majority of absentee votes to be cast as illegal ballots on the unauthorized, non-compliant Optical Scanning System.

123.

All Defendants conducted the election employing procedures that violate essential provisions of the Election Code. Such violations include but are not limited to the following:

124.

First, the Optical Scanning machines were not evaluated prior to the Runoff to determine whether they meet the requirement of Georgia Code Section 21-2-365(8): “It shall, when properly operated, record correctly and accurately every vote cast.”

125.

Second, the Optical Scanning System did not meet the mandatory testing standard provisions of Georgia Code Section 21-2-374(b), which require that the optical scanning tabulators be tested prior to an election to determine whether they count votes accurately. Testing conducted by the state’s Logic and Accuracy Testing did not and could not determine whether the tabulator correctly counted the votes in the Runoff. Only a hand count supervised by this court can make that determination.

126.

Third, in violation of Georgia Code Section 21-2-375(b) and § 21-2-374(a), the superintendents and poll managers failed to provide adequate protection against

“molestation and injury” to the machines when they ordered and accepted programming from CES, whose system they knew to be compromised. The State Board and Secretary Kemp failed to provide adequate rules to assure reasonable security of the equipment and its software, causing the CES equipment and system-wide Optical Scan software and related GEMS programming and databases to be maintained in lax conditions with minimal and ineffective security. Such equipment and programs must be presumed to have been compromised, generating an unreliable result.

127.

Fourth, the tabulation mechanism on the Optical Scanning machines were not secured in compliance with the intent of Georgia Code Section 21-2-377 given the security failures involved in the Optical Scan machine programming. Such security requirements became impossible to meet after the CES system was open to the internet as described in ¶¶ 26 – 47.

128.

Fifth, any new voting system deployed after April 17, 2005 is required to meet the certification standards in Ga. Comp. R. & Regs. 590-8-1-.01. That regulation requires compliance with the most recent Election Assistance Commission (“EAC”) voting standards for certification of a new voting system or substantive change in a previously certified system. On information and belief,

Secretary Kemp has not attempted to certify the system in use to those mandatory state standards, nor has he certified that it meets those standards although the current equipment configuration constitutes a new voting system deployed after April 17, 2005. Yet, on information and belief, Secretary Kemp and King have made misleading public claims before the Runoff that the voting system was “federally and state certified.”

G. Irreparable Harm

129.

Plaintiffs and the Georgia elector members of Plaintiff CGG cannot be adequately compensated for these harms in an action at law for money damages. At equity, Plaintiffs seek—and can obtain only—nominal compensatory relief.

VI. COUNTS

COUNT I: VIOLATION OF ARTICLE II, SECTION I, PARAGRAPH I, OF THE GEORGIA CONSTITUTION OF 1983

**(All Plaintiffs against All Defendants in their Individual Capacities, except
State Board, Fulton Board, DeKalb Board, and Cobb Board)**

Declaratory and Injunctive Relief

O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3

Enjoining Use of Georgia's DRE System and Optical Scanning System

130.

The allegation of paragraphs 1 through 129 above are hereby incorporated as the allegations of this paragraph 130 of Count One of this complaint.

131.

Article II, Section 1, Paragraph 1 of the Georgia Constitution provides, "Elections by the people shall be by secret ballot and shall be conducted in accordance with procedures provided by law."

132.

Elections must be conducted in accordance the statutes and regulations of the State of Georgia.

133.

The Runoff was not conducted in accordance with the “procedures provided by law” because the DRE System was in violation of Georgia Code Section 21-2-379.1(8) at the time of the Runoff. O.C.G.A. § 21-2-379.1(8) provides that DRE Systems “shall, when properly operated [by an elector], register or record correctly and accurately every vote cast.” The Optical Scanning System was similarly in violation of Section 21-2-365(8), which provides that Optical Scanning Systems “shall, when properly operated, record correctly and accurately every vote cast.”

134.

In addition, the DRE System did not and cannot meet additional statutory requirements for safety and accuracy of the equipment. See O.C.G.A. § 21-2-379(b); § 21-2-379.6 (a); § 21-2-379(6)(c); § 21-2-379.7(b); § 21-2-379.7(c); § 21-2-379.7(d)(3); § 21-2-379.9(b). Similarly, the Optical Scanning System did not meet additional statutory requirements for safety and accuracy because of the CES system compromise. See O.C.G.A. § 21-2-365(8); § 21-2-374(a); § 21-2-377. Therefore, Kemp, Members of the State Board, individual County Elections Officials, and King were and are required to remove this equipment from service.

135.

On information and belief, these Defendants knew that these voting systems had been unsecured, breached, and compromised, could not be presumed to be safe, and were materially non-compliant with applicable Election Code statutes and governing regulations. These Defendants were aware of numerous expert opinions advising against the use of these systems in the Runoff election because they were neither safe nor accurate and should have been presumed to be compromised.

136.

Additionally, the Runoff was not conducted in accordance with the “procedures provided by law” because the DRE System used was in violation of Georgia Code Section 21-2-379.2. Georgia Code Section 21-2-379.2(a) requires the Secretary of State to reexamine the DRE voting system, if “[a]ny ten or more electors of this state request the Secretary of State to reexamine any such system previously examined and approved by him or her.” Id. Likewise, the Optical Scanning System used was in violation of Georgia Code Section 21-2-368(a). Georgia Code Section 21-2-368(a) requires the Secretary of State to reexamine the optical scanning voting system, if “[a]ny ten or more electors of this state request the Secretary of State to reexamine any such system previously examined and approved by him or her.” Id.

137.

That was not done here. Concerned about the known system security compromises, Georgia electors repeatedly requested Secretary Kemp to reexamine Georgia's Voting System prior to the Runoff on four separate occasions: on May 10, 17, and 19, and June 2, 2017. Secretary Kemp's office responded on June 5, 2017, stating that reexamining the systems would cost the requesting citizens \$10,000 and take six months. Despite his knowledge of the recent CES system security failures, the stolen pollbooks, the warnings from the FBI, EAC, and DHS, and numerous computer scientists, as well as an escalated risk environment, Secretary Kemp refused to reexamine Georgia's Voting System prior to the Runoff or any currently scheduled 2017 elections.

138.

On July 17, 2017 Secretary Kemp's office responded, agreeing to waive the previously requested \$10,000 fee, but did not agree to reexamine the equipment under the current standards controlling the examination and certification of voting systems. He also did not agree to a timely reexamination prior to Georgia's November 2017 municipal elections, exposing such elections to being illegally conducted and contested.

139.

After a request to examine or reexamine a DRE voting system and the Secretary of State conducts such an examination, “no kind of [DRE] voting system” not approved “shall be used at any primary or election.” O.C.G.A. § 21-2-379.2(c). After a request to examine or reexamine an optical scanning voting system and the Secretary of State conducts such an examination, “no kind of [optical scanning] voting system” not so approved “shall be used at any primary or election.” O.C.G.A. § 21-2-368(c). Furthermore, Georgia’s voting systems must be certified, to ensure that “hardware, firmware, and software have been shown to be reliable, accurate, and capable of secure operation before they are used in elections in the state.” Ga. Comp. R. & Regs. 590-8-1-.01(a)(3). Georgia’s DRE System and Optical Scanning System did not meet these legal requirements, and, further, the DRE System cannot be brought into compliance with these requirements.

140.

Upon reexamination, should it “appear that the [DRE] system... can no longer be safely or accurately used by electors” as provided under the Georgia Code “because of any problem concerning its ability to accurately record or tabulate votes,” then the Secretary of State should “immediately” revoke his approval. O.C.G.A. § 21-2-379.2(c); see also O.C.G.A. § 21-2-368(c) (similar provision governing Optical Scanning Systems). Indeed, given the knowledge

Secretary Kemp and other identified Defendants had of the material non-compliance and insecurity of these systems, Defendants had the duty and authority to act to sideline the compromised systems long before the electors requested system reexamination.

141.

Despite the request for reexamination and the known security failures, the DRE System and Optical Scanning System were used during the Runoff. Secretary Kemp was aware that the security of both systems had been compromised and, for numerous reasons, did not meet certification requirements, statutory requirements, nor be approved as safe or accurate. By choosing to move forward in using the non-compliant system, he willfully and negligently abrogated his statutory duties and abused his discretion, subjecting voters to cast votes on an illegal and unreliable system—a system that must be presumed to be compromised and incapable of producing verifiable results.

142.

Furthermore, when a ballot does not follow a mandate from the Georgia Constitution or the Georgia Code, the ballot is “illegal.” See Count VII; Mead v. Sheffield, 278 Ga. 268, 269 (2004). Such was the case in the Runoff and is expected to be the case in future elections without the intervention of this Court.

143.

Additionally, the identified Defendants violated their duty to recanvass votes under Ga. Comp. R. & Regs. 183-1-12-.02(7)(a), which states that:

The election superintendent shall, either of his or her own motion, or upon petition of any candidate or political party or three electors of the county or municipality, as may be the case, order a recanvass of all the memory cards (PCMCIA cards) for a particular precinct or precincts for one or more offices in which it shall appear that a discrepancy or error, although not apparent on the face of the returns, has been made.

See also Count IV.

144.

These Defendants also violated state equal protection guarantees, as provided in Georgia Constitution's Art. I, Sec. I, Para. II. See Count III. They also violated state due process guarantees. See Count II.

145.

Since these Defendants individually and collectively did not act to ensure the Runoff complied with the "procedures provided by law," as alleged above, they violated the Georgia Constitution, in addition to other applicable Georgia law.

146.

Georgia's DRE System and Optical Scanning System also cannot be legally used in the upcoming Georgia 2017 municipal elections or other future Georgia elections for reasons alleged throughout this Amended Complaint.

147.

On information and belief, despite their knowledge that the DRE System and Optical Scanning System do not comply with the Election Code, these Defendants willfully and knowingly plan to continue to use the non-compliant DRE System and Optical Scanning System in upcoming elections.

148.

Accordingly, pursuant to Georgia Code Section 9-4-2, Plaintiffs pray that this court will declare that these Defendants have violated the Georgia Constitution. Pursuant to Georgia Code Section 9-4-3, Plaintiffs also pray that this court will void *ab initio* the Runoff and the certification of its result because accurate results tabulated in accordance with Georgia law cannot be determined and order a new election to be held as the only just relief available under the laws of Georgia. This court should also enjoin these Defendants' illegal use in future elections of Georgia's DRE System and the illegal use of the Optical Scanning System as it is currently programmed and configured. Finally, this Court should award nominal compensatory relief in the amount of \$1 in recognition of these Defendants' violation of the Georgia Constitution and, as subsequent causation, the rights of Plaintiffs.

COUNT II: VIOLATION OF 42 USC § 1983 – DUE PROCESS

**VIOLATION OF 42 USC § 1983,
DUE PROCESS AND FIRST AMENDMENT**

**(All Plaintiffs against All Defendants in their Official and Individual
Capacities except State Board, Fulton Board, DeKalb Board, and Cobb
Board)**

Declaratory, Injunctive, and Monetary Relief, and Attorneys' Fees

O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3

42 USC § 1983; Fourteenth Amendment; First Amendment

149.

The allegations of paragraphs 1 through 148 above are hereby incorporated as the allegations of this paragraph 149 of Count Two of this complaint.

150.

42 U.S.C. § 1983 provides that “[e]very person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United

States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress”

151.

The failure to comply with the Georgia Constitution and the Georgia Code concerning elections is a violation of federal due process when the patent and fundamental fairness of the election is called into question.

152.

Patent and fundamental fairness of an election is called into question when allegations go well beyond an ordinary dispute over the counting and marking of ballots. Such is the case here, where patent and fundamental unfairness arises from egregious and substantive violations of the Georgia Code and Constitution, causing the election result to be indeterminable.

153.

Elected Georgia government officials—and those they control—denied the electorate the right granted by the Georgia Constitution to choose their elected official in accordance with the procedures provided by state law. Ga. Const. Art. II, § 1, ¶ 2. These state officials include Defendants Secretary Kemp, Members of the

State Board, Barron, Members of the Fulton Board, Daniels, Members of the DeKalb Board, Eveler, Members of the Cobb Board, and King.

154.

These Defendants violated Georgia Code Section 21-2-379.1(8), which provides that any DRE system used in Georgia must, when properly operated by the elector, “record correctly and accurately every vote cast.” Consistent with experts who state that Georgia’s DRE System (and, by logical extension and inference, the Optical Scanning System) must be presumed to have been compromised, it is more than probable that it was compromised prior to the Runoff and that the system could not correctly or accurately count every vote during the Runoff. As a result, the tabulation of the voters’ intent cannot reasonably be known. Central to the franchise of voting is that a vote cast by the elector’s ballot be the vote actually counted. That vote should be reviewable to correct discrepancies in the recording or tabulation process. Even in the contentious case of Bush v. Gore, the entirety of the Supreme Court appeared to agree on this fundamental principle, even as they disagreed on whether procedures that existed in those circumstances violated that principle. See, generally, Bush v. Gore, 531 U.S. 98 (2000) (holding manual recounts ordered by Florida Supreme Court, without specific standards to implement its order to discern “intent of the voter,”

did not satisfy minimum requirement for non-arbitrary treatment of voters necessary, under Equal Protection Clause, to secure fundamental right to vote).

155.

Instead, despite receiving multiple warnings that the DRE System and Optical Scanning System had been compromised—and knowing that that documents capable of enabling a malicious attack were accessed multiple times and downloaded from CES without authorization—Secretary Kemp refused to initiate a review of either system and publicly stated “our system’s secure.”²⁷ These actions amount to a purposeful and willful substantial burdening of the fundamental right to vote and misconduct on his part.

156.

Voters who wish to protect their rights by voting on verifiable paper ballots that are reviewable must undertake burdensome efforts to do so. For example, voters who use paper ballots (absentee ballots) cannot vote in their nearby convenient neighborhood precincts. Voters wishing to vote by paper must take the additional steps to complete an application, receive the application in the mail and fill it out, and mail it several days before an election to ensure receipt on election

²⁷ Kristina Torres, Georgia’s Voting Machines Face Criticism, but State Says They’re Secure, Atlanta Journal Constitution, June 12, 2017, <http://www.myajc.com/news/state--regional-govt--politics/georgia-voting-machines-face-criticism-but-state-says-they-secure/rcxCNafPMorse73l6Gu75M/> (last visited August 2, 2017).

day or travel to the county election office to cast an election-day ballot. Voters wishing to vote with paper ballots with the most timely candidate information available on election day must hand-deliver their ballots to the election office, sometimes involving considerable transportation effort and time, as Curling experienced. Furthermore, those who wish to ensure timely receipt must take the ballot to a county office, not merely mail it. Finally, County and Secretary of State websites do not contain information on deadlines for requesting absentee ballots, making it difficult to learn the process for obtaining and casting absentee ballots. In summary, voting by absentee ballot can involve significant hardship and inconvenience.

157.

Georgia's DRE System and Optical Scanning Systems must be properly certified, reexamined, and approved by the Secretary of State prior to any election, when so requested by ten or more electors. O.C.G.A. § 21-2-379.2(a); § 21-2-368(a); see also Ga Comp. R. & Regs. 590-8-1.01. Here, the Secretary of State did not certify, reexamine or approve the system in compliance with applicable statutes. See Counts I and VIII.

158.

By violating the Georgia Constitution, Georgia's election officials distributed to electors in Georgia's 6th Congressional District an illegal ballot,

precluding their right to vote on a legal ballot in the Runoff. See Counts VI and VII, respectively.

159.

In addition, various board member Defendants who functioned as election “superintendents” violated their duty to recanvass votes upon the request of the electorate. See Count IV.

160.

These Defendants, by burdening the right to vote, violated the Due Process Clause of the Fourteenth Amendment of the U.S. Constitution and the Georgia Constitution’s analogue. U.S. Const. Amend. XIV § 1; Georgia Constitution’s Art. I, § 1, ¶ 1.

161.

By burdening the right to vote, these Defendants violated the First Amendment of the U.S. Constitution. U.S. Const. Amend. I.

162.

Under the circumstances alleged above, relief under 42 U.S.C. § 1983 is warranted. Accordingly, Plaintiffs ask this Court to declare that these Defendants violated the fundamental rights to vote and due process, as well as rights afforded by the Georgia Constitution and Code, of Plaintiffs, declare the Runoff and the certification of its result void *ab initio*, and order a new election to be held as the

only just relief available under the laws of Georgia. This court should also enjoin these Defendants' use of Georgia's DRE System for future elections and the use of the Optical Scanning System until such time as the Optical Scanning System can be fully examined, unauthorized software eliminated, authorized software reinstalled, and the system properly secured. In addition, this Court should award nominal compensatory relief in the amount of \$1, in recognition of these Defendants' violation of applicable federal and state laws and, as subsequent causation, the rights of Plaintiffs. Finally, this Court should award attorneys' fees and costs, as per 42 U.S.C. § 1988, for Defendants' causation of concrete injury to Plaintiffs, whose fundamental right to have their vote counted as cast was thwarted. See also Farrar v. Hobby, 506 U.S. 103 (declaratory, injunctive, and nominal compensatory relief can give rise to attorneys' fees under Section 1988, with courts ultimately "obligated to give primary consideration to the amount of damages awarded as compared to the amount sought") (internal citation omitted).

COUNT III: VIOLATION OF 42 USC § 1983 AND EQUAL PROTECTION

(All Plaintiffs against All Defendants in their Official and Individual Capacities, except State Board, Fulton Board, DeKalb Board, and Cobb Board)

Declaratory, Injunctive, and Monetary Relief, and Attorneys' Fees

O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3

42 USC § 1983; Fourteenth Amendment

163.

The allegations of paragraphs 1 through 162 above are hereby incorporated as the allegations of this paragraph 163 of Count Three of this complaint.

164.

42 U.S.C. § 1983 provides that “[e]very person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be

liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress”

165.

The Equal Protection Clause of the Fourteenth Amendment mandates that “[n]o State shall ... deny to any person within its jurisdiction the equal protection of the laws.” U.S. Const. amend. XIV § 1.

166.

The Plaintiffs who voted using the DRE System are all similarly situated to other registered electors in the Runoff who voted by Optical Scanning System. Furthermore, all Plaintiffs may vote or seek to vote in future Georgia elections using the DRE System and would be similarly situated in such elections to other registered electors who vote by Optical Scanning System.

167.

The Secretary of State and County Boards allowed electors using the Optical Scanning System²⁸ to vote in the Runoff to vote using verifiable, reviewable, and

²⁸ Plaintiffs contend the Optical Scanning System is clearly superior to the DRE System. The Optical Scanning System is, in theory, able to be verified by manual recount, while the DRE System leaves no paper trail at all. As such, it is a superior system, and those who voted using it were permitted to vote in a manner superior to those who were not able to vote using the Optical Scanning System. Plaintiffs note that the Optical Scanning System, while superior to the DRE System, is still illegally deployed and subject to external manipulation, especially when the electronic infrastructure is exposed, as it was in the lead up to the Runoff. The Optical Scanning System is the lesser of two evils, and those who used it were harmed less than those who were forced to use the DRE System.

recountable ballots, although they were cast and tabulated on compromised equipment. These ballots are verifiable and recountable because they can be counted manually in an election contest rather than counted electronically, in a manner necessarily exposed to irregularity, especially given the security failures and non-compliance of the voting systems used. The voters who voted by optical scanning ballots were able to vote in the election using verifiable, recountable ballots, which can be counted, reviewed, and discrepancies corrected under the supervision of this Court, while votes cast in the DRE System are not reviewable against an independent record—thus creating two unequal classes of electors. The Optical Scanning System produces an electronic representation of the ballot, which can be checked against the voter-marked ballot. The DRE System produces only an electronic representation of a vote, with no independent reference document. The voters of the respective ballots have their votes unequally weighted, with greater weighting given to those who voted by optical scanning ballot, whose votes can be verified and errors identified and corrected.

168.

Furthermore, the favorable tabulation and post-election review treatment afforded to those voting through the Optical Scanning System can be accessed only by those who overcome additional hurdles to mitigate their risk of an unverifiable ballot, as compared to those voting by the DRE System. See Count II. Ultimately,

absentee optical scanning ballots and ballots by the DRE-machines are substantially dissimilar in the manner in which they are recorded, processed, counted, and reviewed in Georgia's electoral scheme.

169.

Comparatively, the above-identified Defendants forced electors using the DRE machines in the Runoff to vote unwittingly on ballots for which the tabulation cannot be reviewed or discrepancies corrected by the court in this election contest. These Defendants include Secretary Kemp, Members of the State Board, Barron, Members of the Fulton Board, Daniels, Members of the DeKalb Board, Eveler, Members of the Cobb Board, and King.

170.

As alleged above (see ¶ 155), Secretary Kemp misled the electors, effectively encouraging them to vote on the DRE System on which their votes carried less weight than paper ballot votes

171.

It was "impracticable" to safely use the DRE System given its well-understood multiple violations of the DRE System requirements at § 21-2-379 *et seq.*

172.

In this case, these Defendants had two readily available choices authorized by the Election Code to avoid using an irreparably illegal DRE system. These Defendants could have remediated the existing security issues, properly certified the Optical Scanning System, and then fully employed the Optical Scanning System as authorized by Georgia Code Sections 21-2-366 to -379 or they could have employed hand-counted paper ballots as authorized by Section 21-2-281.

173.

These actions by these Defendants amount to purposeful and willful substantial burdening of the right to vote. See SECSYS, LLC v. Vigil, 666 F.3d 678, 686 (10th Cir. 2012) (Gorsuch, J.) (in Section 1983 action, holding that “[e]ven generally applicable laws initially enacted with entirely proper (non-discriminatory) purposes can themselves later become tools of intentional discrimination in the course of their enforcement.”)

174.

The use of unverifiable, illegal, and improperly constructed ballots in Georgia’s DRE System severely infringed upon these Plaintiffs’ fundamental right to vote by not providing the opportunity to cast a lawful and verifiable vote in accordance with the Georgia Constitution or Code and by Defendants’ misleading the electors with false claims of DRE System security and legal compliance.

The burdens and infringements imposed upon these fundamental rights were differentially imposed upon Optical Scanning System (paper ballot) voters and DRE System (voting computer) voters during the Runoff without justification by any substantial or compelling state interest that could not have been accomplished by other less restrictive means. As the United States Supreme Court has noted, “The right to vote is protected in more than the initial allocation of the franchise. Equal protection applies as well to the manner of its exercise. Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person’s vote over that of another.” Bush, 531 U.S. at 104-105 (2000) (citing Harper v. Virginia Bd. of Elections, 383 U.S. 663, 665 (1966) (“[O]nce the franchise is granted to the electorate, lines may not be drawn which are inconsistent with the Equal Protection Clause of the Fourteenth Amendment.”)) The Supreme Court continued, “It must be remembered that ‘the right of suffrage can be denied by a debasement or dilution of the weight of a citizen’s vote just as effectively as by wholly prohibiting the free exercise of the franchise.’” Id. (quoting Reynolds v. Sims, 377 U.S. 533, 555 (1964)). In this case, Georgia law authorized two alternative systems—(1) the Optical Scanning System, if properly remediated, certified, and implemented or (2) hand-counted paper ballots—that could have been utilized to ensure equal protection of voters.

176.

Even under a rational basis standard, there is no rational basis for unequal treatment of electors predicated on actions in violation of the Georgia Constitution and Code.

177.

Defendant's conduct described herein violated the Fourteenth Amendment right of these Plaintiffs to enjoy equal protection of the law.

178.

In violating the Fourteenth Amendment, Defendant's conduct also violated the Georgia Constitution's Art. I, § 1, ¶ 2, equal protection guarantees, which "are substantially equivalent of equal protection of the laws under the U. S. Constitution." Grissom v. Gleason, 262 Ga. 374, 381 (1992) (emphasis omitted) (citation omitted).

179.

Plaintiffs ask this Court to declare that these Defendants have violated the fundamental right to equal protection of these Plaintiffs and enjoin Defendants from conducting future elections with Georgia's Voting System as currently configured, declare the Runoff and certification of its result void *ab initio*, and order a new election to be held as the only just relief available under the laws of Georgia. Plaintiffs also ask the Court to prohibit the use of Georgia's DRE System

in future elections. In addition, this Court should award nominal compensatory relief in the amount of \$1 in recognition of these Defendants' violation of applicable federal and state laws and, as subsequent causation, the rights of Plaintiffs. Finally, this Court should award attorneys' fees and costs, as per 42 U.S.C. § 1988, for these Defendants' causation of concrete injury to Plaintiffs, whose fundamental right to have their vote counted as cast was and continues to be thwarted.

COUNT IV: FAILURE TO RECANVASS VOTES

(Plaintiff CGG against Defendants Secretary Kemp, Members of State Board, State Board, Daniels, Members of the DeKalb Board, DeKalb Board, Eveler, Members of the Cobb Board, and Cobb Board in their Individual and Official Capacities)

Declaratory and Injunctive Relief

O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3

Ga. Comp. R. & Regs. 183-1-12

180.

The allegations of paragraphs 1 through 179 above are hereby incorporated as the allegations of this paragraph 180 of Count Four of this complaint.

181.

Georgia election rules state: “The election superintendent shall, either of his or her own motion, or upon petition of any candidate or political party or three electors of the county or municipality, as may be the case, order a recanvass of all the memory cards (PCMCIA cards) for a particular precinct or precincts for one or more offices in which it shall appear that a discrepancy or error, although not

apparent on the face of the returns, has been made.” Ga. Comp. R. & Regs. 183-1-12-.02(7)(a).

182.

For the reasons alleged above, Georgia’s DRE System must be presumed to have caused substantial discrepancies or errors in returns, even if not apparent on the face of the returns. Given the fundamental insecurity and lack of auditability of the DRE System, direct evidence of manipulation is not required to establish the substantial likelihood that discrepancies or errors did, in fact, occur in these particular returns.

183.

Plaintiff CGG includes members that petitioned the DeKalb Board and the Cobb Board to recanvass certain precincts in both counties. (See Exhibit M.) The precincts in which recanvassing was sought were selected based on anomalous-appearing results—including extreme swings between purported absentee Optical Scanning System results and purported results.

184.

Defendants Daniels, Members of the DeKalb Board, the DeKalb Board, Eveler, Members of the Cobb Board, and the Cobb Board, despite being presented with a recanvass request which explicitly informed them of their obligation to recanvass the requested precincts, refused to recanvass these precincts. Their

knowing refusal to recanvass represents willful misconduct and abuse of discretion.

185.

On information and belief, Secretary Kemp was informed of these proper requests for recanvassing and the denials of the requests, did not act to permit such recanvassing, and certified the election result, despite his knowledge that voters had concerns about anomalies in identified precincts and voters' rights to recanvass prior to certification had been violated.

186.

Defendants Daniels, Members of the DeKalb Board, the DeKalb Board, Eveler, Members of the Cobb Board, and the Cobb Board willfully violated their duty under Ga. Comp. R. & Regs. 183-1-12-.02(7)(a). Concurrently, these Defendants and Defendant Kemp violated the citizen's right of oversight and review.

187.

Plaintiff CGG prays this court declare that Defendants Daniels, Members of the DeKalb Board, the DeKalb Board, Eveler, Members of the Cobb Board, and the Cobb Board are in violation of their duty to recanvass these precincts permitting electors to explore presumed discrepancies and propose their correction prior to election certification. Plaintiff CGG also prays that this court will void *ab*

initio the Runoff and certification of its result, and declare a new election to be held as the only just relief available under the laws of Georgia.

**COUNT V: LACK OF CERTIFICATION OF DRE SYSTEM AND
OPTICAL SCANNING SYSTEM**

(All Plaintiffs against Defendant Secretary Kemp, in His Individual Capacity)

Declaratory and Injunctive Relief

O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3 and O.C.G.A. § 21-2-379.2

Ga. Comp. R. & Regs. 590-8-1-.01

188.

The allegation of paragraphs 1 through 187 above are hereby incorporated as the allegations of this paragraph 188 of Count Five of this complaint.

189.

Under Georgia law, the Secretary of State is responsible for approving Georgia's voting systems as safe and accurate under the provisions of Georgia Code Section 21-2-379.2 (regarding DRE System) and Section 21-2-368 (regarding Optical Scanning System) certifying Georgia's voting systems under

Ga. Comp. R. & Regs. 590-8-1-.01(d)(7). The purpose of the certification process is to ensure that “hardware, firmware, and software have been shown to be reliable, accurate, and capable of secure operation before they are used in elections in the state.” Id. at (a)(3).

190.

Compliance with the specific provisions of Ga. Comp. R. & Regs. 590-8-1-.01 is required for all voting systems implemented after April 17, 2005, and also for all systems implemented before April 17, 2005 if there has been “a modification to the hardware, firmware, or software of the voting system.” Id. at (b)(4). In such circumstances, under Georgia regulations, the previous State certification becomes invalid. Id.

191.

On information and belief, Secretary Kemp has not properly tested Georgia’s DRE System in its current configuration although significant changes to the system have been implemented since the system was last certified in 2008. Moreover, he has not certified the DRE System in its current form, and the DRE System does not comply with the mandatory requirements of Ga. Comp. R. & Regs. 590-8-1-.01.

192.

The DRE voting system used in Georgia was last certified in May 2008 by then-Secretary Handel. Because various key components and software have been added and modified since, without the required new system certification, the system in use is not certified and, therefore, was not and cannot be used legally.

193.

On information and belief, neither Secretary Kemp nor any previous Secretary of State has ever certified that Georgia's Optical Scanning System "can be safely and accurately used by electors at primaries and elections," as required by Georgia law. O.C.G.A. § 21-2-368(b).

194.

By law, Secretary Kemp must certify any new system configuration, tested as an integrated whole, before it can be used in any election. He has not. Under the provisions of Ga. Comp. R. & Regs. 590-8-1-.01(d), the system must meet current voting systems standards promulgated by the EAC. It does not. Georgia's DRE System and Optical Scanning System as deployed during the Special Election and Runoff were, therefore, illegal. Secretary Kemp, on information and belief, intends to allow the State's election officials continued use of these uncertified systems, including in the upcoming November 2017 municipal elections.

195.

Moreover, Plaintiffs Curling, Price and CGG (then-named Rocky Mountain Foundation) sued Secretary Kemp in this court (2017CV290630) and at the June 7, 2017 hearing, Secretary Kemp produced the history of voting system certifications. A review of that file showed that no certification existed for Georgia's DRE System at the time of the Special Election or Runoff. (See Exhibit K.) Further, the documents of voting system approvals and certifications produced show no approval of the current DRE System declaring that it can be "safely and accurately used" as required by § 21-2-379.2. Additionally, when asked in an open records request to provide documentation of either federal or state certification of the system in use for the Runoff, CES stated that there were no responsive records.

196.

Accordingly, pursuant to Georgia Code Section 9-4-2, Plaintiffs pray that this court will declare that Secretary Kemp has not certified or approved Georgia's DRE System or Optical Scanning System as "safe and accurate" or certified it for use in its present form, a violation of Georgia law. Pursuant to Section 9-4-3, Plaintiffs also pray that this court will enjoin (1) Defendants' use of any configuration of Georgia's DRE System because it cannot meet the previously listed statutory requirements and (2) the use of the Optical Scanning System until such system and its software has been verified and its compliance with Georgia

statutory and constitutional requirements assured via applicable certification and approval.

**COUNT VI: ELECTION CONTEST DUE TO MISCONDUCT AND
IRREGULARITY -- USE OF ILLEGAL, UNSECURED AND/OR
UNCERTIFIED VOTING SYSTEMS**

**(By all Plaintiffs, except Davis, Price, and CGG, against all Defendants in
their Official Capacity, except King)**

**Declaratory and Injunctive Relief
O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3**

O.C.G.A. § 21-2-520

197.

The allegations of paragraphs 1 through 196 above are hereby incorporated as the allegations of this paragraph 197 of Count Six of this complaint.

198.

Under Georgia Code Section 21-2-521, a Contestant is entitled to “contest the result of any primary or election.”

199.

A Contestant can be “any aggrieved elector who was entitled to vote” in an election. O.C.G.A. § 21-2-521. The above-named Plaintiffs were all aggrieved electors in the Runoff. On June 26, 2017, Karen Handel was certified as the winner of the Runoff.

200.

An aggrieved elector has the right to contest the election by naming as a defendant in a lawsuit the “election superintendent or superintendents who conducted the contested primary or election.” O.C.G.A. § 21-2-520(c). Election superintendents include either “the county board of elections [or] the county board of elections and registration,” as the case may be. O.C.G.A. § 21-2-2(35)(A). Additionally, it can include the Secretary of State. See Dawkins-Haigler v. Anderson, 799 S.E.2d 180 (2017). Here, these Plaintiffs named such appropriate defendants.

201.

Since the State and County Boards and their members are “superintendents” under the meaning of this statute, by statute, Defendants State Board, Fulton Board, DeKalb Board, Cobb Board—as well as their respective individual members, including Secretary Kemp as Chair of the State Board, as well as Defendants

Barron, Daniels, and Eveler—lack immunity to an election contest claim. O.C.G.A. § 21-2-520.

202.

The result of any election may be contested if, among other reasons, there is “misconduct, fraud, or irregularity” on the part of any “election official or officials sufficient to change or place in doubt the result.” O.C.G.A. § 21-2-522(1).

203.

Here, the Runoff produced tabulations that are speculative and based on the illogical theory that the non-compliant and undeniably unsecured voting system produced accurate results. The use of Georgia’s DRE System and Optical Scanning System, given their compromised security, material and pervasive non-compliance with the Election Code, and unverifiability of the results, and lack of certification of Georgia’s Voting System as currently configured, amount to an “irregularity” that, at a minimum, “place[s] in doubt” the result of this election. O.C.G.A. § 21-2-522(1); see also Counts I; V (regarding lack of voting system certification for DRE System and Optical Scanning System).

204.

Because the GEMS tabulation server itself was compromised, the tabulation of all ballots has been compromised and the result has been placed in substantial doubt. Moreover, the vast majority of the votes are not capable of verification or

correction of discrepancies. Although the Optical Scanning System ballots, as with the DRE ballots, were improperly counted through electronic means of the Optical Scanning System, they can be recounted and any discrepancies corrected by verifiable means in this proceeding. However, those ballots constitute a small minority of total votes cast. In the Runoff, 260,455 ballots were cast. Of those ballots, approximately 232,712 were cast using the DRE machines. The remaining 27,742 votes were cast by Optical Scanning ballot. 232,712 is significantly greater than the margin of victory in the Runoff – 9,702. Thus, given the extensive use of illegal ballots for which the tabulation cannot be verified, the result of the election is not only placed in substantial doubt, but there is no ability for this court to determine an accurate DRE vote count, recount the DRE ballots, or correct the DRE discrepancies.

205.

Testimony of experts demonstrate their universal agreement that Georgia's DRE System (and, by logical inference and extension, the Optical Scanning System) should not have been used in the Runoff, and cannot be relied on to produce accurate results, placing the election results in significant doubt. (See Exhibits F, G, and H)

206.

Accordingly, these Plaintiffs file this petition to contest the Runoff election result, in addition to their other claims herein. These Plaintiffs pray this court declare this election and the certification of its result void *ab initio* and order a new election to be held as the only just relief available under the laws of Georgia.

**COUNT VII - ELECTION CONTEST DUE TO IRREGULARITY – USE OF
ILLEGAL BALLOTS AND ILLEGAL PROCEDURES**

**(By All Plaintiffs, except Davis, Price, and CGG, against All Defendants in
their Official Capacity, except King)**

**Declaratory and Injunctive Relief
O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3**

O.C.G.A. § 21-2-520

207.

The allegations of paragraphs 1 through 206 above are hereby incorporated as the allegations of this paragraph 207 of Count Seven of this complaint.

208.

Electors in the Runoff used illegal ballots. DRE ballots are illegal because the DRE System on which they were cast is not certified and is in violation of the statutory requirements for such a system and they cannot be cast and tabulated in accordance with the statutory requirements of the Election Code. See O.C.G.A. §§ 21-2-379.1 to -379.12. Absentee ballots used in the Runoff were also illegal because the Optical Scanning System through which they were cast is not certified and is in violation of the statutory requirements for such a system. See O.C.G.A. §§ 21-2-365 to -379. Issuance of illegal ballots are an “irregularity” ordered by “an election official or officials.” O.C.G.A. § 21-2-522(1).

209.

When illegal ballots are used, elector’s choices on the illegal ballots and their purported tabulation is irrelevant. Mead, 278 Ga at 272.

210.

Instead, the question is whether the number of illegal ballots used is “sufficient to change or place in doubt the result” of the election. The number of illegal ballots is sufficient enough to change or place in doubt the result of the election when the amount used by electors to cast their votes is greater than the margin of victory. See Mead 278 Ga. 271.

211.

Because the GEMS tabulation server itself was compromised, the tabulation of ballots has been compromised and the entire results have been placed in doubt.

212.

Moreover, the vast majority of the votes are not capable of verification or subject to the correction of discrepancies. Although the Optical Scanning ballots, as with the DRE ballots, were improperly counted through electronic means, they can be recounted and any discrepancies corrected by verifiable means in this proceeding. However, those ballots constitute a small minority of total votes cast. As stated above, given the extensive use of illegal DRE ballots that cannot be verified, the result of the election is not only placed in substantial doubt, but there is no ability for this court to determine an accurate vote count, to recount the ballots, or to correct discrepancies.

213.

The DRE ballots and the Optical Scanning ballots used in the Runoff were illegal because they did not substantially adhere to the Georgia Constitution or Code. When a ballot does not follow a mandate from the Georgia Constitution or the Georgia Code the ballot is “illegal.” See Mead, 278 Ga. at 269.

214.

Defendants State Board, Fulton Board, DeKalb Board, Cobb Board, as well as their respective individual members, including Secretary Kemp as Chair of the State Board, and Defendants Barron, Daniels, and Eveler, bear statutory responsibility, as “superintendents,” for allowing illegal ballots to be issued, cast and counted under the DRE System and Optical Scanning System. O.C.G.A. § 21-2-520(2)(C). They do not have sovereign or qualified immunity to preclude this claim.

215.

Since the Runoff used illegal ballots in sufficient number to place the election in doubt, including the misconduct and irregularities alleged above, and these Defendants refused to recanvass the votes, the above-named Plaintiffs file this petition to contest the Runoff election result, in addition to their other claims herein. These Plaintiffs pray this court declare the Runoff election and the certification of its result void *ab initio* and declare a new election to be held as the only just relief available under the laws of Georgia.

COUNT VIII: WRIT OF MANDAMUS

(All Plaintiffs against Defendant Secretary Kemp)

Writ of Mandamus

O.C.G.A. § 9-4-3 and O.C.G.A. § 9-4-2; O.C.G.A. § 9-6-20

**Requiring Exercise of the Public Duty to Reexamine Georgia’s DRE System
Established by O.C.G.A. § 21-2-379.2(b) and to Use Optical Scan or Paper
Ballots in Lieu of DRE Machines to Comply with “Safe or Accurate”**

Requirements for Voting Machines

216.

The allegation of paragraphs 1 through 215 above are hereby incorporated as the allegations of this paragraph 216 of Count Eight of this complaint.

217.

Mandamus is a remedy for “government[al] inaction – the failure of a public official to perform a clear legal duty.” Southern LNG, Inc. v. MacGinnitie, 294 Ga. 657, 661 (2014).

218.

Mandamus is warranted when (1) a public official has a clear legal duty to perform an official act (as requested); (2) that the requesting party has a clear legal right to the relief sought or that the public official has committed a gross abuse of discretion; and (3) that there is no other adequate legal remedy. See Bland Farms, LLC v. Georgia Dept. of Agriculture, 281 Ga. 192, 193 (2006); SJN Props., LLC v. Fulton County Bd. of Assessors, 296 Ga. 793, 800 (2015).

219.

The Georgia General Assembly has the power to determine the Secretary of State's clear legal duties. See Ga Const. Art. V, § 3, ¶ 5 (“[T]he General Assembly shall prescribe the powers, duties, compensation, and allowances of... executive officers...”). The General Assembly did so under Georgia Code Section 21-2-50, which requires the Secretary of State to “perform such other duties as may be prescribed by law,” including duties of approving the form of ballots, and developing, programming, and reviewing DRE and Optical Scanning ballots.

220.

One clear duty of the Secretary of State, as prescribed by law, is that “The Secretary of State may, at any time, in his or her discretion, reexamine any [DRE] system.” O.C.G.A. § 21-2-379.2(a). The clear purpose Secretary of State's power to reexamine any DRE system at his discretion is to ensure that the DRE System

can be “safely and accurately used by electors at primaries and elections.”

O.C.G.A. § 21-2-379.2(b). The Secretary of State has the same power, and discretion, to reexamine any Optical Scanning system, with the same purpose of ensuring that such a system be safely and accurately used. O.C.G.A. § 21-2-368.

221.

Although Secretary Kemp was aware of numerous security breaches and statutory non-compliance of the DRE System, he violated his legal obligations by not reexamining Georgia’s DRE System before the Runoff in response to the repeated requests of electors pursuant to Georgia Code Section 21-2-379.2(a)—or abused his discretion by not initiating the reexamination process *sua sponte* before the Runoff pursuant to Section § 21-2-379.2. Secretary Kemp, likewise, violated his legal obligations by not reexamining Georgia’s Optical Scanning System before the Runoff in response to the repeated requests of electors—or abused his discretion by not initiating the reexamination process *sua sponte* before the Runoff. O.C.G.A. § 21-2-368.

222.

Secretary Kemp also violated his duty ultimately upon reexamination – whether requested by electors or *sua sponte* – to remove from commission the DRE System and the Optical Scanning System. If upon reexamination, should it “appear that the system ... can no longer be safely or accurately used by electors”

as provided under the Georgia Code “because of any problem concerning its ability to accurately record or tabulate votes,” then the Secretary of State should “immediately” revoke his approval. O.C.G.A. § 21-2-379.2(c); see also O.C.G.A. § 21-2-368(c) (similar provision with respect to Optical Scanning System). Georgia’s DRE System was not and is not safe or accurate, and its approval for use should have been revoked, if such approval was ever given²⁹; the same is true of the Optical Scanning System. When Secretary Kemp, faced with knowledge of a substantially non-compliant system, failed to take action to revoke and replace Georgia’s Voting System, his inaction left county election officials without a District-wide policy or directive to deploy a legally compliant voting system.

223.

Abuse of discretion is found when a public official acts in an “arbitrary, capricious, and unreasonable” manner. Burke Cty. V. Askin, 291 Ga. 697, 701 (2012) (citing Massey v. Georgia Bd. Of Pardons & Paroles, 275 Ga. 127, 128(2) (2002)). This includes acting in such an arbitrary, capricious way that their abuse

²⁹ That Secretary Kemp never examined the DRE System or the Optical Scanning System in the first place (see Count V) provides no refuge here. The Secretary is obligated to ensure that “No kind of direct recording electronic voting system not so approved shall be used at any primary or election.” O.C.G.A. § 21-2-379.2(c); see also O.C.G.A. § 21-2-368(c) (similar provision with respect to Optical Scanning System). That Kemp failed to properly certify the systems makes his failure to examine in the face of the request and the information about the vulnerability of the systems an even greater abuse of his discretion.

of discretion “amounts to a failure on the part of the officer to exercise his discretion at all.” S. View Cemetery Ass'n v. Hailey, 199 Ga. 478, 483 (1945).

224.

Here, well before the Runoff, Secretary Kemp was informed of at least three breaches into CES system, and was warned by DHS, the FBI, and the EAC that foreign actors were probing multiple states’ election systems, and such agencies of the US government offered specific protective measures for Secretary Kemp to undertake. He was warned repeatedly that Georgia’s DRE System (and, by logical inference and extension, the Optical Scanning System) was highly susceptible to attack based on the allegations stated throughout this Complaint. He was warned by experts at the June 7 hearing (See Curling v. Kemp, Case No. 2017CV290630) that the system could not be used “safely and accurately,” and could not be relied on for accurate results. Although Secretary Kemp admitted that “anything is possible”³⁰ when it comes to Russians tampering with Georgia’s Voting System, he refused to examine the DRE System or the Optical Scanning System for security and compliance.

³⁰ Kim Zetter, Will the Georgia Special Election Get Hacked, Politico, June 14, 2017, <http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255> , (last visited June 30, 2017).

225.

Despite these repeated warnings and breaches, Secretary Kemp, the only top state election official in the nation to do so, refused assistance from the Department of Homeland Security to help protect Georgia's Voting System in August 2016. He did so because he did not "necessarily believe" that hacking of Georgia's elections is a real threat. About the issue he stated, "I think it was a politically calculated move by the [Obama] administration."³¹ His rationale for his belief: "The question remains whether the federal government will subvert the Constitution to achieve the goal of federalizing elections under the guise of security. ... Designating voting systems or any other election system as critical infrastructure would be a vast federal overreach, the cost of which would not equally improve the security of elections in the United States."³²

226.

Such beliefs are arbitrary. They are based on a solely personal belief, unreasonable in that they are not rooted in fact, and contrary to empirically supported concerns expressed to him repeatedly by his constituents, cybersecurity

³¹ Paul Waldman, How Democratic Timidity May Have Helped Trump Get Elected, Washington Post, June 23, 2017, https://www.washingtonpost.com/blogs/plum-line/wp/2017/06/23/how-democratic-timidity-may-have-helped-trump-get-elected/?utm_term=.d36b828f5d08 (last visited July 3, 2017).

³² Allya Sternstein, At Least One State Declines Offer For DHS Voting Security, NextGov, August 25, 2016, <http://www.nextgov.com/cybersecurity/2016/08/some-swing-states-decline-dhs-voting-security-offer/131037/> (last visited July 3, 2017).

experts, voting system experts, the EAC, the FBI, and DHS. His beliefs and reckless decision not to review the system are so arbitrary, capricious, and unreasonable that they “amount[] to a failure on the part of the officer to exercise his discretion at all.” S. View Cemetery Ass’n, 199 Ga. at 483.

227.

Georgia’s DRE System and Optical Scanning System were used in the 2016 General Election, as well as the Special Election, and the Runoff. On information and belief, Secretary Kemp plans to use the systems again in remaining 2017 elections and beyond – despite being more than aware of the burden the systems impose on Georgia electors’ right to vote and of the fact that the systems do not comply with numerous provisions of the Election Code.

228.

The Secretary of State is clearly charged with ensuring the safety and accuracy of Georgia’s Voting System. Yet, Secretary Kemp willfully ignores known threats to Georgia’s election process against the informed counsel of the Federal Government, security experts, voting system experts, and his constituents. His misinformation—and the false assurances he has delivered to the public and elected officials—likely caused voters to use DRE machines based on their mistaken understanding that the DRE System was secure and would properly record their votes. Secretary Kemp essentially did nothing to fulfill his duty to

ensure the legal compliance, safety, and accuracy of Georgia's Voting System but, instead, willfully misled electors by making false claims about the security and certification of the systems in question here. Such reckless inaction and campaign of misinformation constitutes an abuse of discretion. See S. View Cemetery Ass'n., 199 Ga. at 483.

229.

Where the question is one of public right and the object is to procure the enforcement of a public duty, no legal or special interest need be shown, but it shall be sufficient that a plaintiff is interested in having the laws executed and the duty in question enforced. O.C.G.A. § 9-6-24.

230.

The Court has full and complete power to issue mandamus under Georgia Code Section 9-6-20, which provides, “All official duties should be faithfully performed; and whenever, from any cause, a defect of legal justice would ensue from a failure to perform or from improper performance, the writ of mandamus may issue to compel a due performance, if there is no other specific legal remedy for the legal rights.”

231.

Apart from this Court’s issuance of the writ of mandamus, Plaintiffs have no other legal remedy to compel enforcement of Secretary Kemp’s official, public

duty to conduct the reexamination required by Georgia Code Sections 21-2-379.2(b) or 21-2-368(b), nor do they have any other remedy to compel enforcement of Secretary Kemp's duties to remove from commission voting machines that are non-compliant and replace them with a safe, accurate and legally compliant system. Various electors, including Davis, have attempted multiple times to have Secretary Kemp reevaluate the system. However, he has resisted their requests and imposed impractical fees and timelines, when he initially responded, as a reason not to reevaluate. Although he has recently waived the fees to be charged to the requesting electors, he remains unwilling to take timely action. Additionally, Secretary Kemp can act on his own accord. Electors cannot force Secretary Kemp to act in that capacity to fulfill his duties. Only the Court can.

232.

For the reasons provided, Plaintiffs respectfully ask this Court to issue a writ of mandamus for Secretary Kemp to fulfill his public duty to timely reexamine the DRE System and the Optical Scanning System and approve for future elections a legally compliant voting scheme, which, given DRE system's lack of safety and accuracy, must be an optical scan-based system or hand-counted paper ballots.

COUNT IX: WRIT OF MANDAMUS

(All Plaintiffs against Defendants Members of State Board, State Board, Daniels, Members of the DeKalb Board, DeKalb Board, Eveler, Members of the Cobb Board, Cobb Board, Barron, Members of the Fulton Board, and Fulton Board, in their Official Capacities)

Writ of Mandamus

O.C.G.A. § 9-4-3 and O.C.G.A. § 9-4-2; O.C.G.A. § 9-6-20

Requiring Exercise of the Public Duty to Use Optical Scan or Paper Ballots in Lieu of DRE Machines to Comply with “Practicable” Requirements

233.

The allegation of paragraphs 1 through 236 above are hereby incorporated as the allegations of this paragraph 237 of Count Nine of this complaint.

234.

Mandamus is a remedy for “government[al] inaction – the failure of a public official to perform a clear legal duty.” Southern LNG, Inc. v. MacGinnitie, 294 Ga. 657, 661 (2014).

235.

Mandamus is warranted when (1) a public official has a clear legal duty to perform an official act (as requested); (2) that the requesting party has a clear legal right to the relief sought or that the public official has committed a gross abuse of discretion; and (3) that there is no other adequate legal remedy. See Bland Farms, LLC v. Georgia Dept. of Agriculture, 281 Ga. 192, 193 (2006); SJN Props., LLC v. Fulton County Bd. of Assessors, 296 Ga. 793, 800 (2015).

236.

State Board, County Board, and County Election Officials abrogated a duty to remove from use machines that are not practicable. O.C.G.A. § 21-2-334. Again, these Defendants had two readily available choices authorized by the Election Code: they could have fully employed a compliant optical scanning voting system authorized by Georgia Code Section 21-2-366, or they could have used hand-counted paper ballots as authorized by Section 21-2-281. They failed to perform their duty during the Runoff, and without the intervention of his court, such failure is subject to repetition for upcoming elections.

237.

Where the question is one of public right and the object is to procure the enforcement of a public duty, no legal or special interest need be shown, but it

shall be sufficient that a plaintiff is interested in having the laws executed and the duty in question enforced. O.C.G.A. § 9-6-24.

238.

The Court has full and complete power to issue mandamus under Georgia Code Section 9-6-20, which provides, “All official duties should be faithfully performed; and whenever, from any cause, a defect of legal justice would ensue from a failure to perform or from improper performance, the writ of mandamus may issue to compel a due performance, if there is no other specific legal remedy for the legal rights.”

239.

Apart from this Court’s issuance of the writ of mandamus, Plaintiffs have no other legal remedy to compel enforcement of State Board, County Board, and County Election Officials’ official, public duty to remove from commission voting machines that are not “practicable,” and replace them with a safe, accurate and legally compliant system.

240.

For the reasons provided, Plaintiffs respectfully ask this Court to issue a writ of mandamus ordering State Board, County Board, and County Election Officials to discontinue the use of the DRE System and either utilize a fully compliant and

certified optical scanning voting system, pursuant to Georgia Code Section 21-2-366, or, pursuant to Section 21-2-281, use hand-counted paper ballots.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully ask this court:

- to grant declaratory relief deeming that Defendants have violated the Georgia Constitution, 42 U.S.C. § 1983, the Election Code, including Georgia's system certification regulations and provisions, and tabulation, recanvassing and results certification provisions; and declaring the certification of result of the Runoff and the Runoff election itself void *ab initio*;
- to grant declaratory relief deeming that Defendants Daniels, Members of the DeKalb Board, the DeKalb Board, Eveler, Members of the Cobb Board, and the Cobb Board are in violation of their duty to recanvass these precincts permitting electors to explore presumed discrepancies and propose their correction prior to election certification;
- to grant injunctive relief requiring Defendants to conduct a new election as the only just relief available under the laws of Georgia and enjoining all future use of Georgia's DRE System and the future use of the Optical Scanning System as currently configured;

- to issue a writ of mandamus for Secretary Kemp to fulfill his public duty to timely reexamine the DRE System and the Optical Scanning System and approve for future elections a legally compliant voting scheme, which, given DRE system's lack of safety and accuracy, must be an optical scan-based system or hand-counted paper ballots;
- to issue a writ of mandamus for State Board, County Board, and County Election Officials to discontinue the use of the DRE system and either utilize a fully compliant and certified optical scanning voting system or hand-counted paper ballots;
- to grant nominal compensatory damages in the amount of \$1, in recognition of Defendants' violation of applicable federal and state laws, which have caused harm to Plaintiffs;
- to award attorneys' fees and costs for the deprivation of civil rights arising from alleged Defendants' patent and fundamental unfairness in conducting elections on Georgia's Voting System, causing a Section 1983 violation; and
- to grant all other relief this court deems proper.

Respectfully submitted this 4th day of August 2017.

/s/ Bryan M. Ward

Bryan Ward, Esq.

Georgia Bar No. 736656

Marvin Lim, Esq.

Georgia Bar No. 147236

Holcomb + Ward LLP

3399 Peachtree Rd NE, Suite 400

Atlanta, GA 30326

(404) 601-2803 (office)

(404) 393-1554 (fax)

Bryan.Ward@holcombward.com

Marvin@holcombward.com

**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual, et al.)
)
 Plaintiffs,)
)
 v.)
)
 BRIAN P. KEMP, in his individual capacity)
 and his official capacity as Secretary of)
 State of Georgia and Chair of the)
 STATE ELECTION BOARD, et al.,)
)
 Defendants.)

CIVIL ACTION
FILE NO.: 2017cv292233

VERIFICATION OF AMENDED COMPLAINT

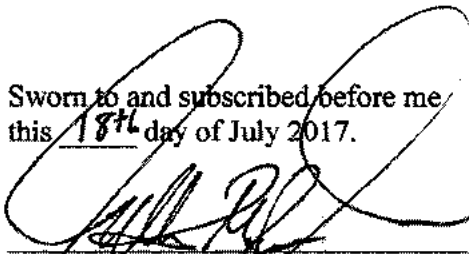
I, **DONNA CURLING**—a plaintiff in the above-styled case—personally appeared before the undersigned notary public who was duly authorized to administer oaths at the time of their signature dated below. In accordance with O.C.G.A. § 21-2-524(d), I affirm the following statements under oath:

1. I petition to contest the result of the Special Election for Georgia's 6th Congressional District between Karen Handel and John Ossoff, held on June 20, 2017 (the "Runoff") in good faith.
2. To my best knowledge and belief, I believe the contested result of the Runoff is illegal and therefore the election return is incorrect.
3. To the best of my knowledge, information, and belief, every fact alleged in the attached Amended Verified Complaint is true and correct, except for any fact that also states a legal conclusion.

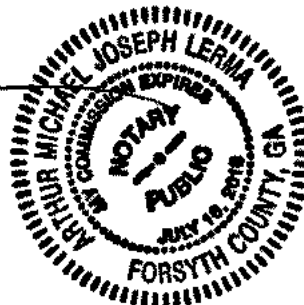
Dated this 18th day of July 2017.


DONNA CURLING

Sworn to and subscribed before me
this 18th day of July 2017.



Notary Public



**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual, et al.)
)
 Plaintiffs,)
)
 v.)
)
 BRIAN P. KEMP, in his individual capacity)
 and his official capacity as Secretary of)
 State of Georgia and Chair of the)
 STATE ELECTION BOARD, et al.,)
)
 Defendants.)

CIVIL ACTION
FILE NO.: 2017cv292233

VERIFICATION OF AMENDED COMPLAINT

I, **MARILYN MARKS**, executive director and an officer of **COALITION FOR GOOD GOVERNANCE**, a plaintiff in the above-styled case, personally appeared before the undersigned notary public, duly authorized to administer oaths, and state under oath that every fact alleged in the **VERIFIED AMENDED COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF, AND WRITS OF MANDAMUS**, attached hereto, is true and correct to the best of my knowledge, information, and belief, except for any fact that also states a legal conclusion.

Dated this 2nd day of ~~July~~ ^{August} 2017.



MARILYN MARKS

Sworn to and subscribed before me
This 2nd day of ~~July~~ ^{August} 2017.

Willetta F. Sullivan
Notary Public

Willetta F. Sullivan
Notary Public
Mecklenburg County, NC

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual, et al.)

Plaintiffs,)

v.)

CIVIL ACTION

FILE NO.: 2017cv292233

BRIAN P. KEMP, in his individual capacity)

and his official capacity as Secretary of)

State of Georgia and Chair of the)


STATE ELECTION BOARD, et al.,)

Defendants.)

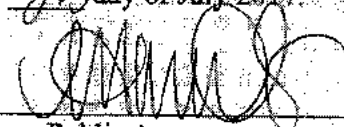
VERIFICATION OF AMENDED COMPLAINT

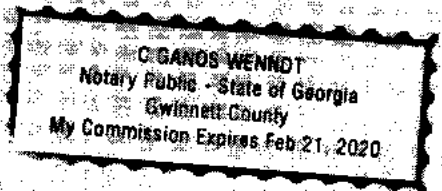
I, **DONNA PRICE**, a plaintiff in the above-styled case, personally appeared before the undersigned notary public, who is duly authorized to administer oaths, and state under oath that every fact alleged in the **VERIFIED AMENDED COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF, AND WRITS OF MANDAMUS**, attached hereto, is true and correct to the best of my knowledge, information, and belief, except for any fact that also states a legal conclusion.

Dated this 20 day of July 2017.


DONNA PRICE

Sworn to and subscribed before me
this 20 day of July 2017.


Notary Public Carol Diaz



**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual, et al.)

Plaintiffs,)

v.)

BRIAN P. KEMP, in his individual capacity)
and his official capacity as Secretary of)
State of Georgia and Chair of the)
STATE ELECTION BOARD, et al.,)

Defendants.)

CIVIL ACTION

FILE NO.: 2017cv292233

VERIFICATION OF AMENDED COMPLAINT

I, **JEFFREY H.E. SCHOENBERG**—a plaintiff in the above-styled case—personally appeared before the undersigned notary public who was duly authorized to administer oaths at the time of their signature dated below. In accordance with O.C.G.A. § 21-2-524(d), I affirm the following statements under oath:

1. I petition to contest the result of the Special Election for Georgia's 6th Congressional District between Karen Handel and John Ossoff, held on June 20, 2017 (the "Runoff") in good faith.
2. To my best knowledge and belief, I believe the contested result of the Runoff is illegal and therefore the election return is incorrect.
3. To the best of my knowledge, information, and belief, every fact alleged in the attached Amended Verified Complaint is true and correct, except for any fact that also states a legal conclusion.

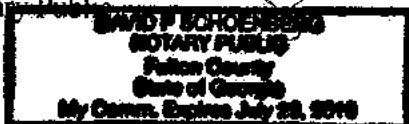
Dated this 18th day of July 2017.



JEFFREY H.E. SCHOENBERG

Sworn to and subscribed before me
this 18th day of July 2017.

Notary Public



**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual, et al.)

Plaintiffs,)

v.)

BRIAN P. KEMP, in his individual capacity)

and his official capacity as Secretary of)

State of Georgia and Chair of the)

STATE ELECTION BOARD, et al.,)

Defendants.)

CIVIL ACTION

FILE NO.: 2017cv292233

VERIFICATION OF AMENDED COMPLAINT

I, **LAURA DIGGES**—a plaintiff in the above-styled case—personally appeared before the undersigned notary public who was duly authorized to administer oaths at the time of their signature dated below. In accordance with O.C.G.A. § 21-2-524(d), I affirm the following statements under oath:

1. I petition to contest the result of the Special Election for Georgia's 6th Congressional District between Karen Handel and John Ossoff, held on June 20, 2017 (the "Runoff") in good faith.
2. To my best knowledge and belief, I believe the contested result of the Runoff is illegal and therefore the election return is incorrect.
3. To the best of my knowledge, information, and belief, every fact alleged in the attached Amended Verified Complaint is true and correct, except for any fact that also states a legal conclusion.

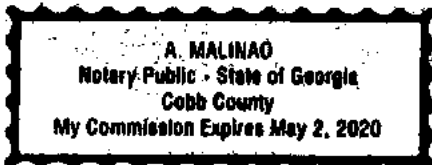
Dated this 18 day of July 2017.


LAURA DIGGES

Sworn to and subscribed before me
this 18 day of July 2017.



Notary Public



Notarization validates
signature only,
not document content.
1

**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual, et al.)

Plaintiffs,)

v.)

BRIAN P. KEMP, in his individual capacity)
and his official capacity as Secretary of)
State of Georgia and Chair of the)
STATE ELECTION BOARD, et al.,)

Defendants.)

CIVIL ACTION

FILE NO.: 2017cv292233

VERIFICATION OF AMENDED COMPLAINT

I, **WILLIAM DIGGES III**—a plaintiff in the above-styled case—personally appeared before the undersigned notary public who was duly authorized to administer oaths at the time of their signature dated below. In accordance with O.C.G.A. § 21-2-524(d), I affirm the following statements under oath:

1. I petition to contest the result of the Special Election for Georgia's 6th Congressional District between Karen Handel and John Ossoff, held on June 20, 2017 (the "Runoff") in good faith.
2. To my best knowledge and belief, I believe the contested result of the Runoff is illegal and therefore the election return is incorrect.
3. To the best of my knowledge, information, and belief, every fact alleged in the attached Amended Verified Complaint is true and correct, except for any fact that also states a legal conclusion.

Dated this 18th day of July 2017.

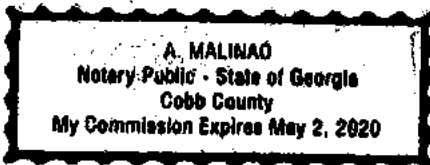


WILLIAM DIGGES III

Sworn to and subscribed before me
this 18 day of July 2017.



Notary Public



Notarization validates
signature only,
not document content.

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual, et al.)
)
 Plaintiffs,)
)
 v.)
)
 BRIAN P. KEMP, in his individual capacity)
 and his official capacity as Secretary of)
 State of Georgia and Chair of the)
 STATE ELECTION BOARD, et al.,)
)
 Defendants.)

CIVIL ACTION
FILE NO.: 2017cv292233

VERIFICATION OF AMENDED COMPLAINT

I, RICARDO DAVIS, a plaintiff in the above-styled case, personally appeared before the undersigned notary public, duly authorized to administer oaths, and state under oath that every fact alleged in the **VERIFIED AMENDED COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF, AND WRITS OF MANDAMUS**, attached hereto, is true and correct to the best of my knowledge, information, and belief, except for any fact that also states a legal conclusion.

Dated this 25 day of July 2017.


RICARDO DAVIS

Sworn to and subscribed before me
this 25th day of July 2017.

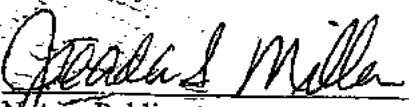

Notary Public

EXHIBIT A

**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual, et al.)

Plaintiffs,)

v.)

BRIAN P. KEMP, in his individual capacity)

and his official capacity as Secretary of)

State of Georgia and Chair of the)

STATE ELECTION BOARD, et al.,)

Defendants.)

CIVIL ACTION
FILE NO.:

AFFIDAVIT OF LOGAN LAMB

County of Fulton)

) ss.

State of Georgia)

LOGAN LAMB ("Affiant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am a cybersecurity researcher based in Atlanta. I have a BS and MS in computer engineering from University of Tennessee, Knoxville. I have worked professionally in cybersecurity since 2010. I started at Oak Ridge National Lab in the Cyber and Information Security Research group. At CISR I specialized in static and symbolic analysis of binaries. I also worked with embedded systems security and conducting security assessments for the federal government. I left ORNL in 2014 and joined Bastille Networks, a local startup where I am still employed. At Bastille Networks I specialize in wireless security and applications of software defined radio.

2. On August 23, 2016 I went to 130 Peachtree Street in an attempt to meet the Fulton County election supervisor Richard Barron with the hope of gaining access to voting systems equipment so that I could conducting a wireless security

assessment as a research project. There I was told to contact Merle King at Kennesaw State University because all election equipment is managed by the Center for Election Systems at KSU.

3. On August 24, 2016 I intended to contact Merle King. Prior to doing so, I wanted to check the Center for Election Systems public website to see if there were any public documents that could give me background on CES and Merle King. I used the search “site:elections.kennesaw.edu inurl:pdf” at www.google.com and discovered what appeared to be files relating to voter registration cached by google.
4. After this discovery, I wrote a quick script to download what public files were available here: <https://elections.kennesaw.edu/sites/> , at the time a publicly accessible site. After running the script to completion I had acquired multiple gigabytes of data. This data was comprised of many different files and formats, but among them were:
 - voter registration databases filled with personally identifiable information of voters (filename *PollData.db3*)
 - Election Management System GEMs databases (.gbf and .mdb extensions)
 - PDFs of election day supervisor passwords, for example:
 - *July 2016 Primary and NP Election Runoff Password Memo.pdf*
 - Windows executables and DLLs, for example:
 - *System.Data.SQLite.DLL*
 - *ExpDbCreate.exe*
 - *ExpReport.exe*
5. Besides leaking information, the server at elections.kennesaw.edu was running a version of Drupal vulnerable to an exploit called drupageddon. Using drupageddon, an attacker can fully compromise a vulnerable server with ease. A

public advisory for drupageddon was release in 2014, alerting users that attackers would be able to execute, create, modify, and delete anything on the server.

On August 28, 2016 I sent an email to Merle King notifying him of the vulnerabilities I found.

Hello Merle,

My name is Logan Lamb, and I'm a cybersecurity researcher who is a member of Bastille Threat Research Team. We work to secure devices against new and existing wireless threats: <https://www.bastille.net/>. This past Tuesday I went to Fulton County Government Center to speak with Rick Barron about securing voting machines against wireless threats. I was then directed to contact you and the center. I'd like to collaborate with you on securing our state's election systems infrastructure against wireless attacks.

While attempting to get more background information on the center prior to contacting you, I discovered serious vulnerabilities affecting elections.kennesaw.edu.

The following google searches reveal documents that shouldn't be indexed and appear to be critical to the elections process. In addition, the Drupal install needs to be immediately upgraded from the current version, 7.31:

"site:elections.kennesaw.edu inurl:pdf"

I generally use this type of search to find documents on websites that lack search functionality. This search revealed a completely open Drupal install. Assume any document that requires authorization has already been downloaded without authorization.

"site:elections.kennesaw.edu L&A"


The second search result appears to be for disseminating critical voting system software. This is especially concerning because, as the following article states, there's a strong probability that your site is already compromised.
<https://www.drupal.org/project/drupalgeddon>
<https://www.drupal.org/SA-CORE-2014-005>

If you have any questions or concerns please contact me. I'm able to come to the center this Monday for a more thorough discussion.

Take care,
Logan

6. After having a brief conversation with Mr. King on August 29, 2016 and being assured that the issues would be remediated, I dropped the issue.

7. In late February, 2017 I told my colleague Chris Grayson about what transpired in August. He quickly confirmed the leaking of information had not been appropriately remediated. I tweaked my script and checked to see if it worked as it had in August.
8. The script was able to download the publicly available information. The data downloaded included the same data from the previous collection and new information relating to recent elections including:
 - More recent GEMs database files
 - Files relating to the presidential election, e.g.
 - *November 2016 General Election Day Password Memo.pdf*
 - *November 2016 General Voter Lookup Password Memo.pdf*
 - Very recent files, e.g. *064 (1-10-2017).pdf*
9. Given the severity and ease with which an attacker can use drupageddon, an attacker would have easily been able to gain full control of the server at elections.kennesaw.edu had they so wanted.
10. Having gained control of the server, an attacker could modify files that are downloaded by the end users of the website, potentially spreading malware to everyone who downloaded files from the website.
11. In addition to the previously mentioned files on the server, there were multiple training videos. One of these training videos instructed users to first download files from the elections.kennesaw.edu website, put those files on a memory card, and insert that card into their local county voting systems.
12. Further Affiant sayeth not.


Logan Lamb

Sworn before me this 30 day of June, 2017, in June.

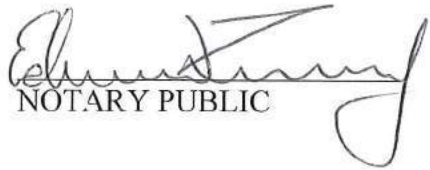

NOTARY PUBLIC



EXHIBIT B

Andino, Marci

From: Brian Newby <BNewby@eac.gov>
Sent: Tuesday, August 23, 2016 4:22 PM
To: John.Merrill@sos.Alabama.gov; stevenreed@mc-ala.org; josie.bahnke@alaska.gov; carol.thompson@alaska.gov; lealofi.uiagalelei@eo.as.gov; fiti.tavai@gmail.com; espencer@azsos.gov; rvalenzuela@risc.maricopa.gov; cpekron@ggtlaw.com; jacksoncountyclerk@gmail.com; Neal.kelley@rov.ocgov.com; dwight.shellman@sos.state.co.us; rsantos@co.weld.co.us; peggy.reeves@ct.gov; tdecarlo@waterburyct.org; elaine.manlove@state.de.us; howard.sholl@state.de.us; Maria.Matthews@DOS.myflorida.com; plux@co.okaloosa.fl.us; bpkemp@sos.ga.gov; lbailey@augustaga.gov; maria.pangelinan@gec.guam.gov; joe.iseke@gec.guam.gov; Aulii.c.tenn@hawaii.gov; Shirley.magarifuji@mauicounty.us; thurst@sos.idaho.gov; pattyweeks@co.nezperce.id.us; bglazier@elections.il.gov; lgough@earthlink.net; bking@lec.in.gov; trethlake@co.st-joseph.in.us; carol.olson@sos.iowa.gov; gveeder@co.black-hawk.ia.us; bryan.caskey@sos.ks.gov; at_county_clerk@wan.kdor.state.ks.us; maryellen.allen@ky.gov; countyclerk@jeffersoncountyclerk.org; Angie.rogers@sos.louisiana.gov; ljperret@lpclerk.com; julie.flynn@maine.gov; KLJ@portlandmaine.gov; Nikki.Charlson@Maryland.gov; katie.brown@maryland.gov; Michelle.Tassinari@sec.state.ma.us; elections@cobma.us; WilliamsS1@michigan.gov; JRoncelli@Bloomfieldtpw.org; gary.poser@state.mn.us; sharon.k.anderson@co.cass.mn.us; Hawley.robertson@sos.ms.gov; bmosley@lafayettecoms.com; julie.allen@sos.mo.gov; Howell@sos.mo.gov; lkimmet@mt.gov; charlotte.mills@gallatin.mt.gov; neal.erickson@nebraska.gov; dshively@lancaster.ne.gov; jwendland@SOS.NV.gov; jpg@ClarkCountyNV.gov; astevens@sos.nh.gov; robertd@pointing.com; Robert.Giles@sos.nj.gov; lvonnessi@aol.com; Kari.Fresquez@state.nm.us; dkunko@co.chaves.nm.us; douglas.kellner@elections.ny.gov; rachel.bledi@albanycounty.com; veronica.degraffenreid@ncsbe.gov; Michael.Dickerson@mecklenburgcountync.gov; jsilrum@nd.gov; cbradley@nd.gov; pwolfe@ohiosecretaryofstate.gov; HARSMANS@mcohoio.org; carol.morris@elections.ok.gov; dousan@oklahomacounty.org; james.r.williams@state.or.us; derrin.robinson@co.harney.or.us; maschneide@pa.gov; jgreenburg@mcc.co.mercer.pa.us; rallende@cee.gobierno.pr; WaValez@cee.gobierno.pr; rrock@sos.ri.gov; Andino, Marci; vr14sblack@hotmail.com; Kristin.Kellar@state.sd.us; jerry.schwarting@state.sd.us; Mark.Goins@tn.gov; astarling@tnaffcio.org; kingram@sos.texas.gov; elections@traviscountytexas.gov; mjthomas@utah.gov; sswensen@slco.org; will.senning@sec.state.vt.us; dorsetclerk@gmail.com; Caroline.Fawkes@vi.gov; genevieve.whitaker@vi.gov; edgardo.cortes@elections.virginia.gov; Griddlemoser@staffordcountyva.gov; stuart.holmes@sos.wa.gov; swansonk@co.cowlitz.wa.us; lbrown@wvsos.com; bwood@putnamwv.org; michael.haas@wi.gov; bgoeckner@village.germantown.wi.us; jgonzales@co.albany.wy.us; kai.schon@wyo.gov

Cc: EAC Leadership
Subject: Attached Security Document
Attachments: BOE_FLASH_aug2016_final.pdf

Dear Standards Board Member,

On behalf of EAC Commissioner Christy McCormick, as the agency's DFO for the Standards Board, I am sending the attached security document to you that has been provided to us recently by the Federal Bureau of Investigation. The FBI has asked that we share this document expressly with election officials.

You'll see that the document identifies specific Internet Protocol (IP) addresses and recommends that election officials scan their systems to ensure these IP addresses are not accessing election systems.

Please share this with other election officials in your state, respecting the FBI's designation that this information be shared on a need-to-know basis only. The attachment is non-classified, but it is not intended for distribution outside of the election administrator community.

Should you have any questions regarding this information, please call or email me. In the meantime, thank you for your assistance regarding this information.

Brian D. Newby, CERA | Executive Director
Election Assistance Commission
1335 East West Highway | Suite 4300
Silver Spring | Maryland | 20910
(301) 563-3959 (O) | (202) 734-0639 (C)
bnewby@eac.gov | www.eac.gov



UNITED STATES
ELECTION ASSISTANCE COM.

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the system manager. The recipient is advised to check this email and any attachments for the presence of viruses. The Election Assistance Commission accepts no liability for any virus transmitted by this email.



FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

18 August 2016

Alert Number
T-LD1004-TT

**WE NEED YOUR
HELP!**

If you find any of these indicators on your networks, or have related information, please contact
**FBI CYWATCH
immediately.**

Email:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released TLP: AMBER: The information in this product is only for members of their own organization and those with DIRECT NEED TO KNOW. This information is NOT to be forwarded on beyond NEED TO KNOW recipients.

Targeting Activity Against State Board of Election Systems

Summary

The FBI received information of an additional IP address, 5.149.249.172, which was detected in the July 2016 compromise of a state's Board of Election Web site. Additionally, in August 2016 attempted intrusion activities into another state's Board of Election system identified the IP address, 185.104.9.39 used in the aforementioned compromise.

Technical Details

The following information was released by the MS-ISAC on 1 August 2016, which was derived through the course of the investigation.

In late June 2016, an unknown actor scanned a state's Board of Election website for vulnerabilities using Acunetix, and after identifying a Structured Query Language (SQL) injection (SQLi) vulnerability, used SQLmap to target the state website. The majority of the data exfiltration occurred in mid-July. There were 7 suspicious IPs and penetration testing tools Acunetix, SQLMap, and DirBuster used by the actor, detailed in the indicators section below.

Indicators associated with the Board of Elections intrusion:

- The use of Acunetix tool was confirmed when "GET /acunetix-wvs-test-for-some-inexistent-file - 443" and several requests with "wvstest=" appeared in the logs;



- The user agent for Acunetix was identified in the logs –
"Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21++(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21";
- The use of SQLMap was confirmed after "GET /status.aspx DLIDNumber=1';DROP TABLE sqlmapoutput" appeared in the logs;
- The user agent for SQLMap is "Mozilla/5.0+(Macintosh;+U;+Intel+Mac+OS+X+10.7;+en-US;+rv:1.9.2.2)+Gecko/20100316+Firefox/3.6.2 200 0 0 421" (These are easily spoofed and not inclusive of all SQLMap activity);
- The user agent for the DirBuster program is "DirBuster-1.0-RC1+(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project<http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project>)";

IP Addresses:

- 185.104.11.154
- 185.104.9.39
- 204.155.30.75
- 204.155.30.76
- 204.155.30.80
- 204.155.30.81
- 89.188.9.91
- 5.149.249.172 (new, per FBI)

Recommendations

The FBI is requesting that states contact their Board of Elections and determine if any similar activity to their logs, both inbound and outbound, has been detected. Attempts should not be made to touch or ping the IP addresses directly.

Recommended Steps for Precautions

The FBI recommends all states take the following precautions to their state Board of Election databases:

- Search logs for commands often passed during SQL injection: SELECT, INSERT, UNION, CREATE, DECLARE, CAST, EXEC, and DELETE, ', %27, –
- Search logs for privilege escalation attempts
 - Looking for references to "cmd.exe" and "xp_cmdshell" (IIS only)
 - Common to see these following SQL injection (logical next step)
 - Can limit search to entries with HTTP status code 200 (success)



- Search for signs of directory enumeration/traversal of the web server file system (used to identify the type of scripting language a web server supports)
 - Looking for series of unsuccessful connections with strange URI strings, such as:
 - GET /Login//..%5c..%5c..%5c..%5c..%5c..%5c..%5cetc/passwd
 - GET /images"OTA2NjAw%40
 - GET /Login//..../etc/passwd
 - GET /Login//..../windows/win.ini
 - Shortly after these requests you should see SQL Injection in the logs
 - May also be "..\..\."

The following recommendations were released by the MS-ISAC on 1 August 2016.

- Conduct vulnerability scans on local government and law enforcement websites and promptly remediate any vulnerabilities (or contact your hosting provider to do so on your behalf). Particular attention should be paid to SQLi vulnerabilities. Website hosting providers should also pay attention to vulnerabilities on other websites on the same server, which may provide a back-door into the local government's website.
- Ensure all software and applications, especially content management software, are fully patched.
- Create custom, general error messages for the web application to generate, as malicious cyber actors can gain valuable information, such as table and column names and data types, through default error messages generated by the database during a SQLi attack.
- Validate user input prior to forwarding it to the database. Only accept expected user input and limit input length. This can be done by implementing a whitelist for input validation, which involves defining exactly what input is authorized.
- Implement the principle of least privilege for database accounts. Administrator rights should never be assigned to application accounts and any given user should have access to only the bare minimum set of resources required to perform business tasks. Access should only be given to the specific tables an account requires to function properly.
- The database management system itself should have minimal privileges on the operating system, and since many of these systems run with root or system level access by default, it should be changed to more limited permissions.
- Isolate the web application from the SQL instructions. Place all SQL instructions required by the application in stored procedures on the database server. The use of user-created stored procedures and prepared statements (or parameterized queries) makes it nearly impossible for a user's input to modify SQL statements because they are compiled prior to adding the input. Also, have the application sanitize all user input to ensure the stored procedures are not susceptible to SQLi attacks.
- Use static queries. If dynamic queries are required, use prepared statements.



- Enable full logging on web servers and email servers to aid in forensic and legal responses if a breach does occur.

Information in this product is for official use only. No portion of this FLASH should be released to the media or the general public. Organizations should not attempt to connect to any of the IP addresses or domain names referenced in this FLASH. The indicators are being provided for network defense purposes only and any activity to these indicators or release of this material could adversely affect investigative activities.

Reporting Notice

The FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to their local FBI Field Office or the FBI's 24/7 Cyber Watch (CyWatch). Field Office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include: the date; time; location; type of activity; number of infected users; type of equipment used for the activity; name of the submitting company or organization; and a designated point of contact.

EXHIBIT C

Zimbra

mking@kennesaw.edu

Re: Vulnerability on the elections.kennesaw.edu website

From : Merle S. King <mking@kennesaw.edu>

Wed, Mar 01, 2017 11:41 PM

Subject : Re: Vulnerability on the elections.kennesaw.edu website**To :** Stephen C. Gay <sgay@kennesaw.edu>

Stephen - We will investigate and advise.

Merle

Sent from my iPad

> On Mar 1, 2017, at 11:10 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:

>

> Merle,

>

> I received the following email, and call, tonight regarding a directory traversal vulnerability on elections.kennesaw.edu. I immediately activated our Incident Response Team and, through the use of burp suite, we were able to recreate the vulnerability described below. In the vulnerability recreation, we were able to pull voter information in database files for counties across the state and the data elements included DOB, Drivers License Number, Party Affiliation, etc. Understanding the risk associated with this vulnerability, we have closed all firewall exceptions for elections.kennesaw.edu to contain the incident. I have asked Bill Moore to act as point for this incident and we need to coordinate with your team on the web logs for elections.kennesaw.edu first thing tomorrow morning. The logs will help us understand the scope of the breach and allow us to advise the CIO as to next steps.

>

> I will be temporarily out of pocket for a short time tomorrow, then remote thereafter, but your cooperation in this incident response is appreciated.

>

> Stephen C Gay CISSP CISA

> KSU Chief Information Security Officer & UITS Executive Director

> Information Security Office

> University Information Technology Services (UITS)

> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu

>
> ----- Forwarded Message -----
> From: "Andy Green" <agreen57@kennesaw.edu>
> To: "Stephen C Gay" <sgay@kennesaw.edu>
> Sent: Wednesday, March 1, 2017 9:55:27 PM
> Subject: Vulnerability on the elections.kennesaw.edu website

> Stephen,

>
> Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a Drupal plug-in vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for directory traversal without authentication, leaving files exposed.

>
> My friend shared with me that the exposed directories contained, among other things:
> - voter registration detail files, including DOB and full SSN.
> - PDFs of memos to county election officials which contained full credentials for ExpressPoll Election Day access, for the November 2016 election.

>
> I was able to verify the presence of the vulnerability myself, and was able to traverse directories without authenticating. I did not download any of the voter data files to verify his statement, for obvious reasons. However, I did successfully open a PDF in my browser window, located in the Fulton County Elections/ExpressPoll/ED_Files/ folder for proof of concept.

>
> The base URL of interest is <http://elections.kennesaw.edu/sites/default/files> - please note that the URL must be http, as use of https will return a 404 error.

>
> I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in

a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.

>

> If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

>

> Thanks

>

> Andy Green, MSIS

>

> Lecturer of Information Security and Assurance

> BBA-ISA program coordinator

> KSU Student ISSA chapter faculty sponsor

> KSU Offensive Security Research Club faculty sponsor

>

> Michael J. Coles College of Business

> Kennesaw State University - A Center of Academic Excellence in Information Assurance Education

> 560 Parliament Garden Way NW, MD 0405

> Kennesaw, GA 30144-5591

> agreen57@kennesaw.edu

> <http://coles.kennesaw.edu/faculty/green-andrew.php>

> Ph: 470-578-4352

> Burruss Building, Room #490

>

> 73656d7065722070617261747573

EXHIBIT D

Background

On Wednesday March 1st at 9:29pm, a member of the KSU UITS Information Security Office was contacted by a KSU faculty member regarding an alleged breach of data on the elections.kennesaw.edu server. UITS staff validated the vulnerability and notified the CIO regarding the incident. The data contained hosted on the identified server was outside the scope of student information and no student records are associated with this alleged breach. Log analysis identified that the largest file identified contained voter registration information for 6.7 million individuals.

Actions Taken

Within an hour of initial contact, the vulnerability was confirmed and firewall rules established to block access to elections.kennesaw.edu. On March 2, 2017, UITS-ISO pulled apache and Drupal logs, reported incident to USG, reset passwords, and seized the elections.kennesaw.edu server. On March 3, 2017, the FBI was engaged and the impacted server was turned over to FBI for investigation.

IT staff which were reporting within the Center for Election systems were realigned to report within the University Information Technology Services Information Security Office and a walkthrough of the area performed to validate the isolated internal network's segregation from the public network. The elections backup server – unicoi – was removed from the Center and physically secured within UITS ISO Evidence Storage.

On March 30th, KSU employees (President Olens, CIO, AVP Strategic Communications, Legal Counsel, CISO, CES Representatives) met with the FBI and US Attorney's Office regarding the outcome of the Federal Investigation. Chad Hunt shared that the investigation had yielded no data that "escalates to the point of breach". KSU Released a statement to the media on 3/31/17 as follows:

KENNESAW, Ga (Mar. 31, 2017) –Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).

University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.

"We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

Financial Impact

None, although if it was determined that the data hosted on elections.kennesaw.edu was maliciously disclosed, the notification and credit monitoring would have been approximately \$2 million.

Successes

The following list describes those actions or systems that worked as intended, or better than anticipated, during the execution of incident and breach response activities:

- The UITS ISO Incident Response process worked as intended, isolating the server and preserving evidence for later analysis and hand-off to federal authorities.
- The time between initial report and the server being isolated was approximately 60 minutes.
- The open dialog between the faculty incident reporter and the Office of the CIO staff facilitated timely notification and rapid response time.
- Having regular conversations with Legal Affairs, Strategic Communications, Center for Election Systems staff, and the Office of the CIO ensured that all parties were informed on developments, allowing for individual planning in each respective area.

Opportunities for Improvement

1. **Issue:** Poor understanding of risk posed by The Center for Election Systems IT systems. While a previous server scan and an external researcher had helped UITS understand the high threat level of CES systems, the lack of understanding the hosted data set led to an incomplete picture of the asset value. This resulted in the existence of a high risk server (High Asset Value / High Threat Level) which should have been prioritized.

Action item(s): An objective 3rd party was hired to conduct a threat assessment for externally-facing applications. In addition, funding was secured to extend the current KSU vulnerability scanning engine to allow for external scans. Once these scans are complete, a thorough analysis of all vulnerable systems will quantify the threat level and remediation plans will be developed (and incorporated into remediation projects)

Action Item Owner(s): UITS Information Security Office

2. **Issue:** Elections webserver and Unicoi backup server are running a vulnerable version of Drupal and vulnerable to exploitation.

Action Items: Elections (externally-facing) was seized immediately and Unicoi (isolated network) was seized thereafter. Both were placed in ISO Secure Storage. UITS provisioned a dedicated virtual server, FS-ES, and business documents were moved to a newly provisioned server. This share is limited the CES subnet and CES Active Directory group users. Server administrators are limited to 2 UITS ISS Staff Members.

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

3. **Issue:** CES confidential data handling processes were not defined.

Action Items: Business processes were developed, documented, and implemented to ensure confidential data is handled appropriately. CES technicians were issued IronKey encrypted hard

drives and secure FTP transfers established with Georgia Secretary of State's Office. To date, all processes have been approved by the Georgia Secretary of State's Office.

Action Item Owner: UITS-ISO, CES Staff, Georgia Secretary of State Office

4. **Issue:** Center for Election System IT staff is not aligned with the University Information Technology Services, creating a scenario in which institutional risk could be accepted without CIO awareness.

Action Items: CES IT staff reporting structure realigned to mirror UITS TSS model. CES IT staff will report directly to UITS-ISO while directly supporting the CES. Additionally, all processes will align with USG and KSU data security policies. Strategically, UITS is launching a project to engage all external IT in order to better understand university-wide IT risk.

Action Item Owner: UITS-ISO, CES Staff

5. **Issue:** Room 105a, the elections private network data closet, was not latching properly due to lock/door misalignment.

Action Items: CISO contacted Chief of Police to have lock and door aligned. Work was completed within one business day. ISO to develop processes to review access logs on a scheduled basis.

Action Item Owner: UITS-ISO, KSU UPD, CES Staff

6. **Issue:** The elections private network data closet contains a live network jack to the [REDACTED] (Public network)

Action Items: UITS-ISO should acquire color-coded Ethernet Jack block-outs to "lock" all ports in the data closet to the public network AND to "lock" all ports to the private network outside the data closet. Key's should be maintained by ISS and ISO, necessitating consulting with UITS staff before connecting devices.

Action Item Owner: UITS-ISO, UITS-ISS

7. **Issue:** A number of IT Assets within the Center for Elections Systems have reached end-of-life and need to be replaced or migrated to different infrastructure.

1. Rackmount UPS Battery backups (one displaying warning light)

Recommendation: Replace batteries as needed and move under UITS ISS management

2. 3com Switches – Age 10+ years -- No Support -- L2 only

Recommendation: Replace and move under UITS ISS management

3. Dell 1950 (Windows Domain Controller) – Age 10+ years

Recommendation: Surplus

4. Dell PowerEdge R630 – Age 1 year

Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network

5. EPIC – Vision Computer – Age Unknown – Ballot creation box

Recommendation: Continue as ISO/CES managed

6. EPIC Files – Dell 1900 – Age 6+ years – Ballot backups

Recommendation: Surplus

7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS

Recommendation: Surplus

8. elections.kennesaw.edu - Age 5 years - Dell PowerEdge R610

Recommendation: Format and reinstall on CES Isolated Network as NAS

9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950

Recommendation: Surplus

10. Web server backup

Recommendation: Surplus

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

8. Issue: An operating system and application security assessment has not been conducted on the CES Isolated Network

Action Items: UITS-ISO should perform a stand-alone security assessment of the CES Isolated Network using a laptop-based scanning engine. Servers and workstations should be hardened based on the scan results and regular testing of the network scheduled.

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

9. Issue: A wireless access point was found when UITS did a walkthrough of the CES House

Action Items: Understanding the risk that a wireless access point presents to the CES isolated network, UITS-ISO should prioritize CES for wireless network upgrade and put guidelines in place which prohibit the use of non-KSU wireless devices in the house.

Action Item Owner: UITS-ISO, UITS-ISS

10. Issue: Inconsistent port colors in House 57. Data outlets throughout the building have different color bezels to indicate which network is public and which is private:

Red = analog voice/phone

Green = KSU data public network

Blue = Elections private network

White = Elections 2nd private network

Since the original cabling installation the two private networks established for elections now act as a single private network. In room 105a, the blue cables terminate to one patch panel and the white cables terminate to another patch panel. They have connected jumpers from both of these patch panels to the same switch thus eliminating any separation by the colors Blue or White.

Action Items: Jacks for the public and private network should be reinstalled to conform to campus color standards. Additionally, jacks from the public and private networks should be on different panels. The total cost of this change will be approximately \$3,000.

Action Item Owner: UITS-ISO, UITS-ISS

EXHIBIT E



From: Michael Barnes mbarne28@kennesaw.edu
Subject: Re: PII found on unicoi.kennesaw.edu (only open to the KSU network)
Date: March 4, 2017 at 7:11 PM
To: Merle S. King mking@kennesaw.edu
Cc: Lectra Lawhorne llawhorn@kennesaw.edu, Stephen C. Gay sgay@kennesaw.edu, sdean29@kennesaw.edu

Unicoi has been shutdown

Michael Barnes
Director
Center for Election Systems
3205 Campus Loop Road
Kennesaw State University
Kennesaw, GA 30144
ph: 470-578-6900

On Mar 4, 2017, at 6:17 PM, Merle S. King <mking@kennesaw.edu> wrote:

Working on it now

--

Merle S. King
Executive Director
Center for Election Systems
3205 Campus Loop Road; MD#5700
Kennesaw State University
Kennesaw, GA 30144
Voice: 470-578-6900
Fax: 470-578-9012

On Mar 4, 2017, at 5:51 PM, Lectra Lawhorne <llawhorn@kennesaw.edu> wrote:

Stephen,

Please call me.

Lec

On Mar 4, 2017, at 5:48 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:

Michael,

Please see below. Can you please shut this server down until we have a chance to meet on Monday to discuss the Center's needs and how best we can work together to meet them? Could you please send conformation of shutdown when completed.

Thank you,
Stephen

Sent from Nine

From: William C. Moore
Sent: Mar 4, 2017 5:44 PM
To: Stephen Gay
Cc: Chris Gaddis
Subject: Fwd: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Stephen

The Core Team is reporting that the Center if Elections server unicoi.kennesaw.edu has files containing PII. One file potentially has 5.7 records and is suspected to be files from 2010.

The server is currently only available from the campus network. We however recommend that the server be removed from the network until all PII data can be secured or removed and verified by the ISO.

Bill

William C. Moore II CISSP, MEd, MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton PI
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

Begin forwarded message:

From: Chris Gaddis <jgaddis6@kennesaw.edu>
Date: March 4, 2017 at 17:32:24 EST
To: "William C. Moore" <wmoore36@kennesaw.edu>
Subject: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Bill,

I noticed that CES brought up Unicoi on Friday (I think its their backup server). Regardless I ran a spider tool on it and found a number of files listed since directory listing is enabled. The top file on this list has 5.7 million records of PII. The rest have a variety of different types of data and some may be completely fine to keep open to the public.

Please note that this server is ONLY open to the KSU network but even still this type of PII should not be open to the KSU network in any form without authentication.

<http://unicoi.kennesaw.edu/sites/default/files/vendors/ESandS/Primary 2010.zip> <---- main concern
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/ExpressPoll/L&AFiles/PollData.db3>
<http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/PollData.db3>
<http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/PollData.db3>
<http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/HD68 Audio.zip>
<http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/022 - Carroll.zip>
<http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/048 - Douglas.zip>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-10-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-100-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/001.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/ballotproof/1-275-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/1-10-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Vote Centers with Cards.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Sign Off Sheet - Ballot Proofs.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-50-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Ballot Order.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-40-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-30-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-20-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-10-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Audio/Sign Off Sheet - Audio Review.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/Reporting Precincts with Cards.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/Reporting Precincts with Cards.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/Documents/Summary Statistics.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-90-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Vote Centers with Cards.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-80-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-70-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Sign Off Sheet - March 15, 2011 Proofs.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Ballot Order.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-60-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-50-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-40-NP-FB.pdf>

<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-30-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-20-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-170-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-160-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-140-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-130-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-120-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-110-NP-FB.pdf>

Let me know if you have any questions about this.

Thanks,

Chris

Chris Gaddis SSCP
Information Security Engineer
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 029
1075 Canton Pl, MB #3503
Kennesaw, GA 30144 USA
Phone: (470) 578-6620
Fax: (470) 578-9050
jgaddis6@kennesaw.edu

EXHIBIT F

**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual, et al.)

Plaintiffs,)

v.)

CIVIL ACTION

FILE NO.:

BRIAN P. KEMP, in his individual capacity)

and his official capacity as Secretary of)

State of Georgia and Chair of the)

STATE ELECTION BOARD, et al.,)

Defendants.)

AFFIDAVIT OF EDWARD W. FELTEN

EDWARD W. FELTEN ("Affiant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am the Robert E. Kahn Professor of Computer Science and Public Affairs at Princeton University, and the Director of Princeton's Center for Information Technology Policy. I received my Ph.D. in Computer Science and Engineering from the University of Washington in 1993. I am a member of the National Academy of Engineering and the American Academy of Arts and Sciences.

2. From 2015 until January 2017, I served in the White House as Deputy United States Chief Technology Officer. During that time I advised the President and his senior advisors on policy issues relating to computer science, including issues relating to the security and reliability of elections and electronic voting systems.

3. A copy of my curriculum vitae is attached as Exhibit A.

Inherent risks of paperless electronic voting machines

4. Before turning to the systems and circumstances specific to Georgia elections, I will provide a brief summary of cybersecurity issues relating to voting machines.

5. The voting machines at issue are a type of so-called Direct Recording Electronic (DRE) machine. DREs are voting machines that are designed to record a voter's ballot directly in electronic storage, without creating any record of the ballot that can be directly verified by the voter.

6. DREs can be contrasted with other voting technologies in which there is a record of the voter's ballot, typically on paper, the accuracy of which can be verified directly by the voter in the polling place, and which is collected at the polling place as a record of the voter's intent. The most common examples of voter-verifiable ballots include paper ballots. Paper ballots can be tabulated by hand counting. Alternatively, they can be tabulated securely by a machine such as an optical scanner, provided that a post-election audit is performed to confirm that the machine count is consistent with the results of manually inspecting a suitable sample of paper ballots.

7. The lack of a voter-verifiable ballot creates special risks associated with any DRE voting system. For this reason, computer scientists and cybersecurity experts typically recommend against the use of DREs. I concur with this general recommendation against the use of DREs.

8. The hardware of a DRE—the physical equipment comprising the computer—is much like a standard desktop computer, often installed into a different physical enclosure. Like a standard computer, a DRE will do whatever the software installed in it directs it to do. If anyone changes the software, whether through malice or error, the DRE may do something other than accurately recording and tabulating votes.

9. A malicious modification to a DRE's software would likely cause the DRE to modify ballots silently. The modified software could be designed to report on the machine's display screen, to voters and election officials, that all was well. It could also be designed to falsify all of the logs and records kept by the voting machine.

10. My students and I have modified the software on many types of DREs. For example, my students modified a (now decommissioned) New York DRE to turn it into a kiosk for playing the popular arcade game Pac-Man. We have also created, installed, and tested software for multiple DRE models that would silently modify election results. (For obvious reasons, these latter tests were done in secure laboratories.)

My team's study of Diebold voting machines

11. I led a team of researchers that studied the Diebold AccuVote TS voting machine system. We published a peer-reviewed paper summarizing our analysis, which is attached as Exhibit B.

12. As part of our research we demonstrated that it was possible to create a voting machine virus: a computer virus that infected the voting machines, spreading from machine to machine by infecting the memory cards that are used to transport election and ballot information between the machines and central tabulation offices. The virus, having infected a voting machine, would modify election results, without leaving any trace in the logs or records kept by the machine. We created and tested such a virus in our secure laboratory.

13. The voting machine virus we created could spread from machine to machine even though the machines were never connected to any network. The virus would spread by infecting memory cards that were transported between machines. When a memory card was inserted into an infected machine, the virus would infect the memory card. When an infected memory card was inserted into a previously unaffected machine, the virus would infect this machine. Thus the memory cards acted as carriers for the virus, much as mosquitoes act as carriers for some human diseases.

14. The notion that machines not connected to the Internet are somehow immune to viruses or other security compromise is a fallacy. It is inconsistent with decades of experience with cybersecurity. In the specific case of Georgia voting machines, it is directly disproven by the research in my laboratory.

15. I did a live demonstration of this election-stealing virus, including showing the casting of votes and mis-reporting of the vote counts by the machine, during live testimony at a hearing of a committee of the U.S. House of Representatives. My students and I did a similar demonstration twice on live television, on CNN and Fox News.

16. The TS machine we studied allowed modified (and possibly malicious) software to be installed by anyone who could open a small metal access door on the side of the machine. The door was locked by an ordinary file cabinet type of lock. Because the very same key that is used for the access door on the AccuVote TS is also used widely on office furniture, jukeboxes, and hotel minibars, the keys are easily purchased. I bought a gross of these keys (i.e., 144 keys) from a vendor on the Internet. The lock is also easily picked—a member of our team who studies locks as hobby was able to pick the access door lock consistently in less than 15 seconds.

17. In short, we demonstrated that a person with access to a TS machine can modify its software, and that this modification can render the machine unable to accurately record or tabulate votes.

18. Our peer reviewed paper listed a number of other security problems with the AccuVote TS system. Some of these problems could in principle be fixable by improving the software of the TS, but others are inherent in the machine's hardware and therefore not fixable by any software update.

19. As described in our peer reviewed paper, it is inherent in the hardware design of the TS that a person who can get physical access to the inside of the machine can install any software they like on the machine.

20. In short, we demonstrated that a person with access to a TS machine can modify its software, and that this modification can render the machine unable to accurately record or tabulate votes. This problem is inherent in the hardware design of the TS machine.

21. Subsequent to the publication of our paper, we studied the AccuVote TSX system and found that it had similar security problems.

Need for software verification

22. One cannot know that any DRE machine, including a TS or TSX, will accurately record or tabulate votes, unless one is certain as to which software is installed on that machine. Because of the ease of malicious modification of the software, it is not enough to know which software is supposed to be installed—one must inspect the machine to verify which software is actually installed.

23. Verifying which software is actually installed is technically very difficult, because one cannot rely on the software itself to report its own status accurately. Malicious software can simply misreport its own status, reporting that everything is normal. Relying on the software to report whether it has been tampered with is like trying to determine whether a person is honest by asking him, “Are you honest?” An answer of “yes” is not reliable evidence.

24. Unfortunately, the standard methods for inspecting the software version installed in a machine rely on the machine’s software in one way or another, so they fail to avoid this pitfall and should not be trusted. Special protocols, typically involving the use of specialized equipment, must be designed and used to perform such inspections, and rigorous chain-of-custody controls are necessary after the inspection to make sure no tampering with the machine’s software could have occurred after the inspection.

25. Unless all of these steps are followed, with respect to a particular DRE machine, one cannot be confident in its ability to accurately record or tabulate votes.

Need for secure facilities

26. I understand that Georgia voting machines are tested and configured in the Center for Election Systems (CES) at Kennesaw State University (KSU). Because my team’s research has demonstrated the propagation of malicious software during these types of activities, including propagation to systems not directly connected to the Internet, any security breach at CES, or failure to implement adequate cybersecurity precautions at CES, could have created an opportunity for a malicious party to modify software in voting machines and related systems.

27. The security breach at CES, and KSU’s response to it, are indications that cybersecurity precautions at CES may not have been adequate. It is significant that KSU’s response to the breach included steps to change how cybersecurity and system administration were managed at CES, so that CES personnel were no longer managing these functions on their own. It is significant that the post-breach report from KSU’s Information Security Office listed as its first “Opportunit[y] for Improvement” the “Poor understanding of risk posed by [CES] IT systems.”

28. The most sophisticated cyberattackers are especially skilled not only at gaining unauthorized access to systems, but also at maintaining access. So-called Advanced Persistent Threat actors specialize in gaining access and maintaining that access over time, while avoiding detection and waiting for the best moment to strike. Once they are in a system, it can be extraordinarily difficult to find them. As a result, very stringent measures may be necessary to

render a facility safe after a period of vulnerability—and especially when highly skilled actors may have been motivated to compromise that facility.

29. Because of the vulnerability of the DRE voting machines to software manipulation, and because of intelligence reports about highly skilled cyber-actors having attempted to affect elections in the United States, such precautions appear to be indicated for the CES systems. In the absence of stringent precautions to find and expel potential intruders in the CES systems, the ability of voting-related systems that have been in the CES facility to function correctly and securely should be viewed with greater skepticism.

30. Further Affiant sayeth not.



Edward W. Felten

State of New Jersey
County of Mercer

Taylor J Cerverizzo, Notary Public



Edward W. Felten

Education

Ph.D. in Computer Science and Engineering, University of Washington, 1993.

Dissertation title: "Protocol Compilation: High-Performance Communication for Parallel Programs." Advisors: Edward D. Lazowska and John Zahorjan.

M.S. in Computer Science and Engineering, University of Washington, 1991.

B.S. in Physics, with Honors, California Institute of Technology, 1985.

Employment

Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University, 2013-present

Deputy United States Chief Technology Officer, The White House, Office of Science and Technology Policy, 2015-2017

Professor of Computer Science and Public Affairs, Princeton University, 2006-2013.

Chief Technologist, U.S. Federal Trade Commission, 2011-2012.

Professor of Computer Science, Princeton University, 2003-2006.

Associate Professor of Computer Science, Princeton University, 1999-2003.

Assistant Professor of Computer Science, Princeton University, 1993-99.

Senior Computing Analyst, Caltech Concurrent Computing Project, California Institute of Technology, 1986-1989.

Director, Center for Information Technology Policy, Princeton University, 2005-present.

Elysium Digital LLC and various law firms. Consulting and expert testimony in technology litigation, 1998-2015

U.S. Federal Trade Commission: consulting regarding spam policy and investigation, 2004, 2006.

U.S. Dept. of Justice, Antitrust Division: consulting and testimony in Microsoft antitrust case, 1998-2002..

Electronic Frontier Foundation. Consulting in intellectual property / free speech lawsuits, 2001-2010.

Certus Ltd.: consultant in product design and analysis, 2000-2002.

Cigital Inc.: Technical Advisory Board member, 2000-2007.

Cloakware Ltd.: Technical Advisory Board member, 2000-2003.

Propel.com: Technical Advisory Board member, 2000-2002.

NetCertainty.com: Technical Advisory Board member, 1999-2002.
FullComm LLC: Scientific Advisory Board member, 1999-2001.
Sun Microsystems: Java Security Advisory Board member, 1997-2001.
Finjan Software: Technical Advisory Board member, 1997-2002.
International Creative Technologies: consultant in product design and analysis, 1997-98.
Bell Communications Research: consultant in computer security research, 1996-97.

Honors and Awards

National Academy of Engineering, 2013.
Alumni Achievement Award, University of Washington, 2013.
American Academy of Arts and Sciences, 2011.
E-Council Teaching Award, School of Engineering and Appl. Sci., Princeton, 2010.
ACM Fellow, 2007.
EFF Pioneer Award, 2005.
Scientific American Fifty Award, 2003.
Alfred P. Sloan Fellowship, 1997.
Emerson Electric, E. Lawrence Keyes Faculty Advancement Award, Princeton University School of Engineering, 1996.
NSF National Young Investigator award, 1994.
Outstanding Paper award, 1997 Symposium on Operating Systems Principles.
Best Paper award, 1995 ACM SIGMETRICS Conference.
AT&T Ph.D. Fellowship, 1991-93.
Mercury Seven Foundation Fellowship, 1991-93.

Research Interests

Information security. Privacy. Technology law and policy. Internet software.
Intellectual property policy. Using technology to improve government. Operating systems. Distributed computing. Parallel computing architecture and software.

Professional Service

Professional Societies and Advisory Groups

ACM U.S. Public Policy Council, Chair, 2014-2015.
ACM U.S. Public Policy Committee, Vice Chair, 2008-2010, 2012-2014.
DARPA Privacy Panel, 2010-2012.
Transportation Security Administration, Secure Flight Privacy Working Group, 2005.
National Academies study committee on Air Force Information Science and Technology Research, 2004.
Electronic Frontier Foundation, Advisory Board, 2004-2007.
ACM U.S. Public Policy Committee, 2004-present (Executive Committee, 2005-present)

ACM Advisory Committee on Security and Privacy, 2002-2003.
DARPA Information Science and Technology (ISAT) study group, 2002-2004.
Co-chair, ISAT study committee on “Reconciling Security with Privacy,” 2001-2002.
National Academy study committee on Foundations of Computer Science, 2001-2004.

Program Committees

World Wide Web Conference, 2006.
USENIX General Conference, 2004.
Workshop on Foundations of Computer Security, 2003.
ACM Workshop on Digital Rights Management, 2001.
ACM Conference on Computer and Communications Security, 2001.
ACM Conference on Electronic Commerce, 2001.
Workshop on Security and Privacy in Digital Rights Management, 2001.
Internet Society Symposium on Network and Distributed System Security, 2001.
IEEE Symposium on Security and Privacy, 2000.
USENIX Technical Conference, 2000.
USENIX Windows Systems Conference, 2000.
Internet Society Symposium on Network and Distributed System Security, 2000.
IEEE Symposium on Security and Privacy, 1998.
ACM Conference on Computer and Communications Security, 1998.
USENIX Security Symposium, 1998.
USENIX Technical Conference, 1998.
Symposium on Operating Systems Design and Implementation, 1996.

Boards

Verified Voting, Advisory Board, 2013-present.
Electronic Privacy Information Center, Advisory Board, 2013-present.
Electronic Frontier Foundation, Board of Directors, 2007-2010.
DARPA Information Science and Technology study board, 2001-2003.
Cigital Inc.: Technical Advisory Board (past).
Sun Microsystems, Java Security Advisory Council (past).
Cloakware Ltd.: Technical Advisory Board (past).
Propel.com: Technical Advisory Board (past).
Finjan Software: Technical Advisory Board (past).
Netcertainty: Technical Advisory Board (past).
FullComm LLC: Scientific Advisory Board (past).

University and Departmental Service

Council on Teaching and Learning, 2014-2015.
School of Engineering and Appl. Sci., Strategic Plan Steering Committee, 2014-2015
Committee on Online Courses, 2012-2013.
Director, Center for Information Technology Policy, 2005-present.
Committee on the Course of Study, 2009-present.
SEAS Strategic Planning, 2004.
 Member, Executive Committee
 Co-Chair, Interactions with Industry area.

Co-Chair, Engineering, Policy, and Society area.
Faculty Advisory Committee on Policy, 2002-present.
Council of the Princeton University Community, 2002-present (Executive Committee)
Faculty Advisory Committee on Athletics, 1998-2000.
Computer Science Academic Advisor, B.S.E. program, class of 1998 (approx. 25 students)
Faculty-Student Committee on Discipline, 1996-98.
Faculty-Student Committee on Discipline, Subcommittee on Sexual Assault and Harrassment, 1996-98.

Students Advised

Ph.D. Advisees:

Harlan Yu (Ph.D. 2012). Dissertation: Designing Software to Shape Open Government Policy. Founder, Upturn Partners.

Ariel J. Feldman (Ph.D. 2012). Dissertation: Privacy and Integrity in the Untrusted Cloud. Assistant Professor of Computer Science, University of Chicago.

Joseph A. Calandrino (Ph.D. 2012). Dissertation: Control of Sensitive Data in Systems with Novel Functionality. Consulting Computer Scientist, Elysium Digital.

William B. Clarkson (Ph.D. 2012). Dissertation: Breaking Assumptions: Distinguishing Between Seemingly Identical Items Using Cheap Sensors. Technical staff member at Google.

Matthias Jacob (Ph.D. 2009). Technical staff member at Nokia.

J. Alex Halderman (Ph.D. 2009). Dissertation: Security Failures in Non-traditional Computing Environments. Associate Professor of Computer Science, University of Michigan.

Shirley Gaw (Ph.D. 2009). Dissertation: Ideals and Reality: Adopting Secure Technologies and Developing Secure Habits to Prevent Message Disclosure. Technical staff member at Google.

Brent Waters (Ph.D. 2004). Dissertation: Security in a World of Ubiquitous Recording Devices. Professor of Computer Science, University of Texas.

Robert A. Shillingsburg (Ph.D. 2004). Dissertation: Improving Distributed File Systems using a Shared Logical Disk. Retired; previously a technical staff member at Google.

Michael Schneider (Ph.D. 2004). Dissertation: Network Defenses against Denial of Service Attacks. Researcher, Supercomputing Research Center, Institute for Defense Analyses.

Minwen Ji (Ph.D. 2001). Dissertation: Data Distribution for Dynamic Web Content. Researcher, HP Labs.

Dirk Balfanz (Ph.D. 2000). Dissertation: Access Control for Ad Hoc Collaboration. Technical staff member at Google.

Dan S. Wallach (Ph.D. 1998). Dissertation: A New Approach to Mobile Code Security. Professor of Computer Science, Rice University.

Significant Advisory Role:

Drew Dean (Ph.D. 1998). Advisor: Andrew Appel. Research Scientist, SRI International.

Stefanos Damianakis (Ph.D. 1998). Advisor: Kai Li. President and CEO, Netrics, Inc.

Pei Cao (Ph.D. 1996). Advisor: Kai Li. Technical staff at Facebook.

Lujo Bauer (Ph.D. 2003). Advisor: Andrew Appel. Associate Professor, School of Computer Science, Carnegie Mellon University.

Publications

Books and Book Chapters

- [1] The Economics of Bitcoin, or Bitcoin in the Presence of Adversaries. Joshua A. Kroll, Ian Davey, and Edward W. Felten. To appear, Lecture Notes in Computer Science series.
- [2] Enabling Innovation for Civic Engagement. David G. Robinson, Harlan Yu, and Edward W. Felten. In *Open Government*, Daniel Lathrop and Laurel Ruma, eds., O'Reilly, 2010.
- [3] *Securing Java: Getting Down to Business with Mobile Code*. Gary McGraw and Edward W. Felten. John Wiley and Sons, New York 1999.
- [4] *Java Security: Web Browsers and Beyond*. Drew Dean, Edward W. Felten, Dan S. Wallach, and Dirk Balfanz. In "Internet Besieged: Countering Cyberspace Scofflaws," Dorothy E. Denning and Peter J. Denning, eds. ACM Press, New York, 1997.
- [5] *Java Security: Hostile Applets, Holes and Antidotes*. Gary McGraw and Edward Felten. John Wiley and Sons, New York, 1996
- [6] Dynamic Tree Searching. Steve W. Otto and Edward W. Felten. In "High Performance Computing", Gary W. Sabot, ed., Addison Wesley, 1995.

Journal Articles

- [7] Accountable Algorithms. Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu. University of Pennsylvania Law Review, Vol. 165, 2017. *Forthcoming. 2016 Future of Privacy Forum Privacy Papers for Policymakers Award*.
- [8] Government Data and the Invisible Hand. David Robinson, Harlan Yu, William Zeller, and Edward W. Felten. *Yale Journal of Law and Technology*, vol. 11, 2009.
- [9] Mechanisms for Secure Modular Programming in Java. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. *Software – Practice and Experience*, 33:461-480, 2003.
- [10] The Digital Millennium Copyright Act and its Legacy: A View from the Trenches. *Illinois Journal of Law, Technology and Policy*, Fall 2002.
- [11] The Security Architecture Formerly Known as Stack Inspection: A Security Mechanism for Language-based Systems. Dan S. Wallach, Edward W. Felten, and Andrew W. Appel. *ACM Transactions on Software Engineering and Methodology*, 9:4, October 2000.

- [12] Statically Scanning Java Code: Finding Security Vulnerabilities. John Viega, Tom Mutdosch, Gary McGraw, and Edward W. Felten. *IEEE Software*, 17(5), Sept./Oct. 2000.
- [13] Client-Server Computing on the SHRIMP Multicomputer. Stefanos N. Damianakis, Angelos Bilas, Cezary Dubnicki, and Edward W. Felten. *IEEE Micro* 17(1):8-18, February 1997.
- [14] Fast RPC on the SHRIMP Virtual Memory Mapped Network Interface. Angelos Bilas and Edward W. Felten. *IEEE Transactions on Parallel and Distributed Computing*, February 1997.
- [15] Implementation and Performance of Integrated Application-Controlled File Caching, Prefetching and Disk Scheduling. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. *ACM Transactions on Computer Systems*, Nov 1996.
- [16] Virtual Memory Mapped Network Interface Designs. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, Kai Li, and Malena Mesarina. *IEEE Micro*, 15(1):21-28, February 1995.

Selected Symposium Articles

- [17] Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. *IEEE Symposium on Security and Privacy*, 2015.
- [18] A Precautionary Approach to Big Data Privacy. Edward W. Felten, Joanna Huey, and Arvind Narayanan. *Conference on Privacy and Data Protection*, 2015.
- [19] On Decentralizing Prediction Markets and Order Books. Jeremy Clark, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Andrew Mill, and Arvind Narayanan. *Workshop on Economics of Information Security*, May 2014.
- [20] Mixcoin: Anonymity for Bitcoin with Accountable Mixes. Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. *Proceedings of Financial Cryptography*, February 2014.
- [21] Privacy Concerns of Implicit Security Factors for Web Authentication. Joseph Bonneau, Edward W. Felten, Prateek Mittal, and Arvind Narayanan. *Adventures in Authentication: WAY Workshop*, 2014.
- [22] The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. Joshua Kroll, Ian Davey, and Edward W. Felten. *Workshop on the Economics of Information Security*, 2013.
- [23] Social Networking with Friendegrity: Privacy and Integrity with an Untrusted Provider. Ariel J. Feldman, Aaron Blankstein, Michael J. Freedman, and Edward W. Felten. *Proc. USENIX Security Symposium*, Aug. 2012.
- [24] Bubble Trouble: Off-Line De-Anonymization of Bubble Forms. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. *Proc. USENIX Security Symposium*, Aug. 2011

- [25] You Might Also Like: Privacy Risks of Collaborative Filtering. Joseph A. Calandrino, Ann Kilzer, Arvind Narayanan, Edward W. Felten, and Vitaly Shmatikov. Proc. IEEE Symposium on Security and Privacy, May 2011.
- [26] SPORC: Group Collaboration Using Untrusted Cloud Resources. Ariel J. Feldman, William P. Zeller, Michael J. Freedman, and Edward W. Felten. Proc. Symposium on Operating Systems Design and Implementation, 2010.
- [27] SVC: Selector-Based View Composition for Web Frameworks. William Zeller and Edward W. Felten. Proc. USENIX Conference on Web Application Development, 2010.
- [28] Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs. Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. Alex Halderman, Christopher J. Rossbach, Brent Waters, and Emmet Witchel. Proc. 17th Network and Distributed System Security Symposium, 2010.
- [29] Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage. Stephen Checkoway, Ariel J. Feldman, Brian Kantor, J. Alex Halderman, Edward W. Felten, and Hovav Shacham. Proc. Electronic Voting Technology Workshop, 2009.
- [30] Some Consequences of Paper Fingerprinting for Elections. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2009.
- [31] Software Support for Software-Independent Auditing. Gabrielle A. Gianelli, Jennifer D. King, Edward W. Felten, and William P. Zeller. Proc. Electronic Voting Technology Workshop, 2009.
- [32] Fingerprinting Blank Paper Using Commodity Scanners. William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten. Proc. ACM Symposium on Security and Privacy, May 2009.
- [33] Lest We Remember: Cold Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Proc. Usenix Security Symposium, 2008.
- [34] In Defense of Pseudorandom Sample Selection. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2008.
- [35] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.
- [36] Machine-Assisted Election Auditing. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.
- [37] Lessons from the Sony CD DRM Episode. J. Alex Halderman and Edward W. Felten. Proc. Usenix Security Symposium, 2006.

- [38] A Convenient Method for Securely Managing Passwords. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. Proc. 14th World Wide Web Conference, 2005.
- [39] New Client Puzzle Outsourcing Techniques for DoS Resistance. Brent R. Waters, Ari Juels, J. Alex Halderman, and Edward W. Felten. ACM Conference on Computer and Communications Security. November 2004.
- [40] Privacy Management for Portable Recording Devices. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. 3rd Workshop on Privacy in Electronic Society. November 2004.
- [41] Receiver Anonymity via Incomparable Public Keys. Brent R. Waters, Edward W. Felten, and Amit Sahai. ACM Conference on Computer and Communications Security. November 2003.
- [42] Attacking an Obfuscated Cipher by Injecting Faults. Matthias Jacob, Dan Boneh, and Edward W. Felten. ACM Workshop on Digital Rights Management, November 2002.
- [43] A General and Flexible Access-Control System for the Web. Lujo Bauer, Michael A. Schneider, and Edward W. Felten. 11th USENIX Security Symposium, August 2002.
- [44] Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design. Batya Friedman, Daniel C. Howe, and Edward W. Felten. Hawaii International Conference on System Sciences, January 2002. (Best Paper award, organizational systems track.)
- [45] Reading Between the Lines: Lessons from the SDMI Challenge. Scott A. Craver, John P. McGregor, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward W. Felten. USENIX Security Symposium, August 2001.
- [46] Cookies and Web Browser Design: Toward Realizing Informed Consent Online. Lynette I. Millett, Batya Friedman, and Edward W. Felten. Proc. of CHI 2001 Conference on Human Factors in Computing Systems, April 2001.
- [47] Timing Attacks on Web Privacy. Edward W. Felten and Michael A. Schneider. Proc. of 7th ACM Conference on Computer and Communications Security, Nov. 2000.
- [48] Archipelago: An Island-Based File System for Highly Available and Scalable Internet Services. USENIX Windows Systems Symposium, August 2000.
- [49] Proof-Carrying Authentication. Andrew W. Appel and Edward W. Felten. Proc. of 6th ACM Conference on Computer and Communications Security, Nov. 1999.
- [50] An Empirical Study of the SHRIMP System. Matthias A. Blumrich, Richard D. Alpert, Yuqun Chen, Douglas W. Clark, Stefanos, N. Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, Margaret Martonosi, Robert A. Shillner, and Kai Li. Proc. of 25th International Symposium on Computer Architecture, June 1998.
- [51] Performance Measurements for Multithreaded Programs. Minwen Ji, Edward W. Felten, and Kai Li. Proc. of 1998 SIGMETRICS Conference, June 1998.

- [52] Understanding Java Stack Inspection. Dan S. Wallach and Edward W. Felten. Proc. of 1998 IEEE Symposium on Security and Privacy, May 1998.
- [53] Extensible Security Architectures for Java. Dan S. Wallach, Dirk Balfanz, Drew Dean, and Edward W. Felten. Proc. of 16th ACM Symposium on Operating Systems Principles, Oct. 1997. Outstanding Paper Award.
- [54] Web Spoofing: An Internet Con Game. Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Proc. of 20th National Information Systems Security Conference, Oct. 1997.
- [55] Reducing Waiting Costs in User-Level Communication. Stefanos N. Damianakis, Yuqun Chen, and Edward W. Felten. Proc. of 11th Intl. Parallel Processing Symposium, April 1997.
- [56] Stream Sockets on SHRIMP. Stefanos N. Damianakis, Cezary Dubnicki, and Edward W. Felten. Proc. of 1st Intl. Workshop on Communication and Architectural Support for Network-Based Parallel Computing, February 1997. (Proceedings available as Lecture Notes in Computer Science #1199.)
- [57] Early Experience with Message-Passing on the SHRIMP Multicomputer. Richard D. Alpert, Angelos Bilas, Matthias A. Blumrich, Douglas W. Clark, Stefanos Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, and Kai Li. Proc. of 23rd Intl. Symposium on Computer Architecture, 1996.
- [58] A Trace-Driven Comparison of Algorithms for Parallel Prefetching and Caching. Tracy Kimbrel, Andrew Tomkins, R. Hugo Patterson, Brian N. Bershad, Pei Cao, Edward W. Felten, Garth A. Gibson, Anna R. Karlin, and Kai Li. Proc. of 1996 Symposium on Operating Systems Design and Implementation.
- [59] Java Security: From HotJava to Netscape and Beyond. Drew Dean, Edward W. Felten, and Dan S. Wallach. Proc. of 1996 IEEE Symposium on Security and Privacy.
- [60] Integrated Parallel Prefetching and Caching. Tracy Kimbrel, Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1996 SIGMETRICS Conference.
- [61] Software Support for Virtual Memory-Mapped Communication. Cezary Dubnicki, Liviu Iftode, Edward W. Felten, and Kai Li. Proc. of Intl. Parallel Processing Symposium, April 1996.
- [62] Protected, User-Level DMA for the SHRIMP Network Interface. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996
- [63] Improving Release-Consistent Shared Virtual Memory using Automatic Update . Liviu Iftode, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996
- [64] Synchronization for a Multi-Port Frame Buffer on a Mesh-Connected Multicomputer. Bin Wei, Gordon Stoll, Douglas W. Clark, Edward W. Felten, and Kai Li. Parallel Rendering Symposium, Oct. 1995.

- [65] A Study of Integrated Prefetching and Caching Strategies. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1995 ACM SIGMETRICS Conference. Best Paper award.
- [66] Evaluating Multi-Port Frame Buffer Designs for a Mesh-Connected Multicomputer. Gordon Stoll, Bin Wei, Douglas W. Clark, Edward W. Felten, Kai Li, and Patrick Hanrahan. Proc. of 22nd Intl. Symposium on Computer Architecture.
- [67] Implementation and Performance of Application-Controlled File Caching. Pei Cao, Edward W. Felten, and Kai Li. Proc. of 1st Symposium on Operating Systems Design and Implementation, pages 165-178, November 1994.
- [68] Application-Controlled File Caching Policies. Pei Cao, Edward W. Felten, and Kai Li. Proc. of USENIX Summer 1994 Technical Conference, pages 171-182, 1994.
- [69] Virtual Memory Mapped Network Interface for the SHRIMP Multicomputer. Matthias A. Blumrich, Kai Li, Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Jonathan S. Sandberg. Proc. of Intl. Symposium on Computer Architecture, 1994.
- [70] Performance Issues in Non-Blocking Synchronization on Shared-Memory Multiprocessors. Juan Alemany and Edward W. Felten. Proceedings of Symposium on Principles of Distributed Computing, 1992.
- [71] Improving the Performance of Message-Passing Applications by Multithreading. Edward W. Felten and Dylan McNamee. Proceedings of Scalable High-Performance Computing Conference (SHPCC), 1992.
- [72] A Highly Parallel Chess Program. Edward W. Felten and Steve W. Otto. 1988 Conference on Fifth Generation Computer Systems.

Selected Other Publications

- [73] Testimony for Privacy and Civil Liberties Oversight Board hearing on “Defining Privacy”. November 2014. Written testimony submitted December 2014.
- [74] Heartbleed Shows Government Must Lead on Internet Security. Edward W. Felten and Joshua Kroll. *Scientific American*, July 2014.
- [75] How the NSA Piggy-Backs on Third-Party Trackers. Edward Felten and Jonathan Mayer. *Slate*, Dec. 13, 2013.
- [76] Testimony for Senate Judiciary Committee hearing on “Continued Oversight of the Foreign Intelligence Surveillance Act,” October 2, 2013.
- [77] The Chilling Effects of the DMCA. Edward Felten. *Slate*, March 29, 2013.
- [78] CALEA II: Risks of Wiretap Modifications to Endpoints. [20 authors]. Submitted to a White House working group.
- [79] Strangers in a Strange Land. Review of *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion*, by Abelson, Ledeen, and Lewis. *American Scientist*, 97:4. July/August 2009.

- [80] Lest We Remember: Cold-Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. *Communications of the ACM*, 52(5):91-98. May 2009.
- [81] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Sept. 2006.
- [82] Digital Rights Management, Spyware, and Security. Edward W. Felten and J. Alex Halderman, *IEEE Security and Privacy*, Jan./Feb. 2006.
- [83] Inside RISKS: DRM and Public Policy. Edward W. Felten. *Communications of the ACM*, 48:7, July 2005.
- [84] Understanding Trusted Computing: Will its Benefits Outweigh its Drawbacks? Edward W. Felten. *IEEE Security and Privacy*, May 2003.
- [85] A Skeptical View of DRM and Fair Use. Edward W. Felten. *Communications of the ACM* 46(4):56-61, April 2003.
- [86] Consumer Privacy and Government Technology Mandates in the Digital Media Marketplace. Testimony before U.S. Senate Commerce Committee. September 2003.
- [87] Secure, Private Proofs of Location. Brent R. Waters and Edward W. Felten. Submitted for publication, 2003.
- [88] An Efficient Heuristic for Defense Against Distributed Denial of Service Attacks using Route-Based Distributed Packet Filtering. Michael A. Schneider and Edward W. Felten. Submitted for publication, 2003.
- [89] Written testimony to House Commerce Committee, Subcommittee on Courts, the Internet, and Intellectual Property, oversight hearing on "Piracy of Intellectual Property on Peer to Peer Networks." September 2002.
- [90] Written testimony to Senate Judiciary Committee hearings on "Competition, Innovation, and Public Policy in the Digital Age: Is the Marketplace Working to Protect Digital Creativity?" March 2002.
- [91] Informed Consent Online: A Conceptual Model and Design Principles. Batya Friedman, Edward W. Felten, and Lynette I. Millett. Technical Report 2000-12-2, Dept. of Computer Science and Engineering, University of Washington, Dec. 2000.
- [92] Mechanisms for Secure Modular Programming in Java. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. Technical Report CS-TR-603-99, Department of Computer Science, Princeton University, July 1999.
- [93] A Java Filter. Dirk Balfanz and Edward W. Felten. Technical Report 567-97, Dept. of Computer Science, Princeton University, October 1997.
- [94] Inside RISKS: Webware Security. Edward W. Felten. *Communications of the ACM*, 40(4):130, 1997.
- [95] Simplifying Distributed File Systems Using a Shared Logical Disk. Robert A. Shillner and Edward W. Felten. Princeton University technical report TR-524-96.

- [96] Contention and Queueing in an Experimental Multicomputer: Analytical and Simulation-based Results. Wenjia Fang, Edward W. Felten, and Margaret Martonosi. Princeton University technical report TR-508-96.
- [97] Design and Implementation of NX Message Passing Using SHRIMP Virtual Memory Mapped Communication. Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Kai Li. Princeton University technical report TR-507-96.
- [98] Protocol Compilation: High-Performance Communication for Parallel Programs. Edward W. Felten. Ph.D. dissertation, Dept. of Computer Science and Engineering, University of Washington, August 1993.
- [99] Building Counting Networks from Larger Balancers. Edward W. Felten, Anthony LaMarca, and Richard Ladner. Univ. of Washington technical report UW-CSE-93-04-09.
- [100] The Case for Application-Specific Communication Protocols. Edward W. Felten. Univ. of Washington technical report TR-92-03-11.
- [101] A Centralized Token-Based Algorithm for Distributed Mutual Exclusion. Edward W. Felten and Michael Rabinovich. Univ. of Washington technical report TR-92-02-02.
- [102] Issues in the Implementation of a Remote Memory Paging System. Edward W. Felten and John Zahorjan. Univ. of Washington technical report TR-91-03-09.

EXHIBIT G

AFFIDAVIT OF DUNCAN A. BUELL

DUNCAN A. BUELL, being duly sworn, deposes and says the following under penalty of perjury.

1. I am a professor of Computer Science and Engineering at the University of South Carolina. I submit this affidavit in support of the petition to void the June 20, 2017, election and to prohibit further use of Georgia's current DRE voting system..

2. In my opinion, the Diebold electronic voting system used in Georgia is vulnerable both to malicious interference and inadvertent error. The Diebold system in general has been put under technical scrutiny several times by technical experts, and each time there have been multiple concerns raised about security and reliability. In fact, each laboratory attempt to compromise DRE systems to change votes has been successful.

3. The possible stamp of approval (for a modified system?) given by the Kennesaw State University (KSU) Center for Election Systems (CES) does not in my opinion mitigate for use in Georgia the known flaws of the system. Indeed, the recent reports from the Kim Zetter article for *Politico* seem to demonstrate that the KSU CES has been either unable or unwilling to address security, privacy, and integrity issues even when they have been privately disclosed to the CES by credible cybersecurity professionals. The fact that the FOIA request of Mr. Garland Favorito yielded only three emails between CES and Mr. Logan Lamb and Mr. Christopher Grayson suggests further that CES might not have been taking seriously the security threats that were pointed out by Lamb and Grayson.

Qualifications and Relevant Employment History

4. In 1971, I earned a B.S. in Mathematics from the University of Arizona. The following year, I earned an M.A. in Mathematics from the University of Michigan. In 1976, I earned a doctorate in Mathematics, with an emphasis in number theory, from the University of Illinois at Chicago. A copy of my resume is available on my university website at <http://www.cse.sc.edu/duncanbuell>.

5. Since 2000, I have been a Professor in the Department of Computer Science and Engineering at the University of South Carolina. From 2000 to 2009, I served as Chair of that department. During 2005-2006, I served as Interim Dean of the College of Engineering and Information Technology at the University of South Carolina. In my management capacity as department chair, my duties also included the management of the college's information technology staff and its network and computer center, which included 9 instructional labs with approximately 250 desktop computers. I was also responsible for the management and operation of cluster computers, file and mail servers, and the college's network infrastructure.

6. Prior to 2000, I was for just under 15 years employed (with various job titles and duties) at the Supercomputing Research Center (later named the Center for Computing Sciences) of the Institute for Defense Analyses, a Federally Funded Research and Development Center (FFRDC) supporting the National Security Agency. Our mission at SRC/CCS was primarily to conduct research on high performance computing systems and computational mathematics to ensure that those computing systems would be suitable for use by NSA, since the NSA workload has technical characteristics

different from most high-end computations like weather modeling. While at IDA I played a leading role in a group that received a Meritorious Unit Citation from Director of Central Intelligence George Tenet for what was then “the largest single computation ever made” in the U.S. intelligence community.

7. In 2013, I was elected a Fellow of the American Association for the Advancement of Science. In 2016, I was appointed to the NCR Chair in Computer Science and Engineering at the University of South Carolina.

8. My current research interests include electronic voting systems, digital humanities, high performance computing applications, parallel algorithms and architecture, computer security, computational number theory, and information retrieval. Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured on each of these topics.

9. Since about 2004 I have been working with the League of Women Voters of South Carolina (LWVSC) as an unpaid consultant on the issue of electronic voting machines. South Carolina uses statewide the ES&S iVotronic terminals and the corresponding Unity software. Beginning in summer 2010, I worked with citizen volunteer activists Frank Heindel, Chip Moore, Eleanor Hare, and Barbara Zia on acquisition by FOIA of the election data from the November 2010 general elections in South Carolina and on the analysis of that data. That work, based on data we acquired by FOIA, culminated in an academic paper that was presented at the annual USENIX EVT/WOTE (Electronic Voting Technology Workshop/Workshop on Trustworthy Elections) conference in August 2011. My work with the LWVSC has continued. When

the state of South Carolina acquired the 2010 election data from the counties and posted it on the SCSEC website, I analyzed that data as well. I have obtained and analyzed the data from the 2012, 2014, and 2016 elections in South Carolina, and I have also analyzed ES&S DRE-voting system data in more limited quantities from Colorado, North Carolina, Pennsylvania, and Texas.

Basis for My Opinions

10. I base the opinions in this affidavit on my knowledge, skill, training, education, and experience: I have been programming computers for more than 45 years and have been employed as a computer scientist for more than 35 years, working with computers and computer applications and operations and management of large computer networks, including file and mail servers that utilize the Internet.

11. I have also used for my opinions a review of the documents surrounding the KSU CES hack in Spring 2017, including the report attached to an email on 24 April 2017 from Stephen Gay to Merle King.

The Diebold Election System Was Unacceptable for Use in the CD6 Election Held 20 June 2017

12. I begin with the fact that the security, reliability, and software quality flaws of the standard Diebold election system are well known to everyone in the computer security world who has an interest in election systems. The letter from Georgia citizens to Secretary of State (SoS) Brian Kemp on 10 May 2017 cites the security analysis of

Feldman, Halderman, and Felten. The GEMS central server software analysis by Ryan and Hoke, cited in the same letter, shows flaws in the central server. The fact that all analyses of the “standard” Diebold election system, even operated in intended conditions, have found major flaws should cause all Georgia voters to have grave concerns as to whether the known failings and vulnerabilities have been mitigated for use in Georgia elections.

13. Evidence indicates that the April 18 and June 20 Special Elections were conducted using a “non-standard” customized Diebold DRE voting system, with an unusual configuration, not tested by a federally accredited laboratory.

14. Even more alarming is the fact that the CES server containing crucial election programming files was known to be open to entry and manipulation in August 2016, and this glaring security problem had not been corrected even as late as March 1, 2017.

15. We must assume that the failure to secure the system and its data caused the already unreliable and unfit system unquestionably to be vulnerable to undetected attack. The system must be considered compromised and it is only prudent that the system must be considered to have been compromised from August 2016 through March 2017, and should not be used to conduct a public election.

16. It has been well-established in the computer security world that the Diebold election system, as configured for “standard” use, is unfit for use due to security and reliability concerns. In my letter/request to Secretary Kemp, serving as a technical advisor to the citizens of Georgia who had petitioned for the non-use of the Diebold

systems in the 20 June 2017 election, I asked for responses to the questions of security and reliability. If the standard system had been modified by CES, and that system had been re-certified, and one could rely upon the security credentials of the KSU CES, then one might have some limited confidence in the suitability of the Diebold system for use in elections in Georgia.

17. The response from Secretary Kemp has been tepid at best. His letter of June 5, 2017, does not address technical questions, and does not really address the questions posed by the electors of Georgia in their original request to him.

18. To be specific, the report of 18 April 2017, attached to Mr. Gay's email to Merle King, is damning in what it says and what it does not say. What we see as "successes" are only that the response to a security incident went well. This is essentially the statement that when law enforcement officials arrived at the barn, they found the door closed, and they found no horses inside the barn, but they had arrived quickly.

19. We see a number of issues in the 18 April 2017 report that indicate that the KSU CES security protocols were insufficient, and we find no commentary on any of those protocols that might have mitigated the damage.

20. I do not see that there are technical comments about successful, or positive, security measures that would have mitigated the potential damage done by the fact that the CES system was apparently open to attack for an extended period by any determined actor.

21. Indeed, the report can be read to suggest that the CES was not following some of the most basic security practices taught to all undergraduates in a computer

security course. Issues 1 and 8, under “Opportunities for Improvement”, for example, cite a poor understanding of risk and of asset value on a main server and a failure to perform a security assessment. This apparent failure to know and to understand basic principles of security would not be inconsistent with Mr. Lamb’s account that sensitive data was still openly available months after he had notified CES of this major security problem.

22. We come to the bottom line. We know, because it has been shown repeatedly, that the Diebold system as it is standardly configured, has major flaws. We would believe, based on our knowledge of process in Georgia, that it is the responsibility of the KSU CES to mitigate (or perhaps even remove?) these major flaws. But we do not see, in the report regarding the operational practices of the CES, that there is reason to believe that they have in fact mitigated the known flaws, produced a system that has been federally or state certified, and provided to the citizens of Georgia an election system in which they can be confident. For these reasons, the voting system in use cannot reasonably be approved as “safe and accurate for use” as required by Georgia statute.

23. For these reasons, I would argue that the Diebold system ought not be used in elections unless and until a complete security analysis has been performed on the software and hardware and a complete verification and integrity check has been made of the databases, including voter registration databases. Nor should the reported results generated by the system be relied on for a determination of the outcome of the June 20 special election.

24. I affirm that the foregoing is true and correct.



DUNCAN BUELL

Date

Sworn before me this 29th day of June, 2017, in Columbia, SC.

Rebecca Mayo
NOTARY PUBLIC

EXHIBIT H

**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual, et al.)	
)	
Plaintiffs,)	
)	
v.)	CIVIL ACTION
)	FILE NO.: 2017cv292233
BRIAN P. KEMP, in his individual capacity)	
and his official capacity as Secretary of)	
State of Georgia and Chair of the)	
STATE ELECTION BOARD, et al.,)	
)	
Defendants.)	

DECLARATION OF BARBARA SIMONS

BARBARA SIMONS ("Declarant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am computer scientist. I was a Research Staff Member at IBM Research. I subsequently worked as a researcher at IBM's Application Development Technology Institute, followed by time working as a Senior Technical Advisor at IBM Global Services.
2. I am the past Chair and current President of Verified Voting. I am also a former President of the Association for Computing Machinery, the world's largest and oldest educational and scientific computing society.
3. I co-authored *Broken Ballots: Will Your Vote Count?*, a book on voting technology. I wrote the chapter on Diebold that lists the many studies that repeatedly demonstrated the insecurities of Diebold DREs.
4. My curriculum vitae is attached as Exhibit A.

Opinions of other experts

5. I have reviewed the affidavit of Edward Felten filed with this court on July 3, 2017 and reviewed the basic structure of Georgia's DRE-based voting system. I concur

with the facts and opinions regarding Georgia's voting DRE voting system as presented in the Felten affidavit.

6. I have reviewed the affidavit of Duncan Buell dated June 29, 2017 and filed with this court on July 3, 2017. I concur with the facts and opinions regarding Georgia's DRE-voting system as presented in the Buell affidavit.

Background related to Georgia's 6th District Congressional Elections

7. Upon learning of the March 1, 2017 compromise of the Center for Election Systems servers containing sensitive election files, I helped to organize the March 15, 2017 letter to Secretary of State Kemp from 21 technology experts expressing our serious concerns regarding the safety and accuracy of Georgia's DRE-based voting system. (Exhibit B.)
8. After the April 15, 2017 alleged theft of poll books and the April 18 Fulton County memory card uploading issues, I helped to organize the May 24, 2017 follow up letter from 16 technology experts to Secretary Kemp expressing our grave concerns about the escalating risks of Georgia's paperless voting system, and urged the use of paper ballots. (Exhibit C.)
9. The information published in the June 14, 2017 Politico article (<http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255>) concerning the long-term exposed nature of the CES server and its contents was alarming to me, furthering my grave concerns about Georgia's voting system.
10. I have reviewed Logan Lamb's affidavit concerning his access to the system and filed with this court July 3, 2017.
11. The facts leading up to the 2017 created an undeniable necessity for Georgia's election officials to conduct the April 18 and June 20 special elections presuming that the DRE-based system had been compromised and could not be reasonably relied on for a valid election.
12. I was gravely disappointed that Secretary Kemp and Georgia's 6th Congressional District election officials chose not to conduct verifiable elections with paper ballots after the serious warnings of numerous respected voting system experts.
13. I have researched DRE voting systems since 2003.

14. I have published my research with consistent findings that DRE machines cannot produce a reliable, auditable, re-countable results that provide assurance that voter intent is recorded and tabulated.
15. I concur with the findings of the National Institute of Standards and Technology (NIST) in their January, 2011 report on the work of the Auditability Working Group of the Technical Guidelines Development Committee prepared for the Election Assistance Commission.
https://www.eac.gov/assets/1/28/AuditabilityReport_final_January_2011.pdf
16. Of particular importance and applicability to Georgia's Special Elections is the NIST Executive Summary statement: "The Auditability Working Group found no alternative that does not have as a likely *consequence* either an effective requirement for paper records or the possibility of undetectable errors in the recording of votes."
17. The "likely consequence" of undetectable errors in Georgia's unverifiable voting results became all the more likely when fundamental security requirements were violated by Georgia officials, causing the results of the recent elections to be unreliable.


Opinions related to use of DRE's in the 6th Congressional District Special Elections

18. The possibility and plausibility of undetectable errors has always existed in Georgia's DRE-based system. However, the risk of undetected and undetectable errors has been exponentially increased by the fact that the system has shown to be exposed to cybersecurity threats at an unexpected level.
19. The cybersecurity threats are heightened not only by the extreme risk caused by the inexplicably lax security at CES, but by the routine practices in Georgia of exposing memory cards and GEMS to equipment connected to the internet, and by lax physical security practices in storage of DRE machines when not in use.
20. The multiple security lapses must be presumed to have caused undetectable manipulation of the tabulation results, which cannot be viewed with any reasonable degree of certainty.

21. Georgia's DRE equipment used in the Special Elections could not be reasonably evaluated prior to the Special Elections to determine whether the votes can be read correctly and accurately.
22. County level and precinct level election officials cannot fulfill their duty to determine that the DRE machines have no votes recorded on them before each machine is opened for voting. That is because the voting machines are essentially computers. Computers consist of distinct elements, such as the display (the screen), the memory, and the input mechanism (in this case the touch screen). These elements communicate via communication channels. If a computer's software (firmware) contains software bugs or malicious software, the computer memory could store votes for Candidate A before the election begins, but the software (firmware) could instruct the printer to print wrongly that no votes have been recorded.
23. It is quite unlikely that standard physical security procedures in place in Georgia can prevent the operation of the "counting machinery" when it is stored and not in use. The "counting machinery" is subject to undetectable manipulation through physical or electronic intrusion.
24. County and precinct election officials charged with the duty to determine whether the machines count votes accurately cannot use the pre-election Logic and Accuracy Testing to make this determination because it is possible to detect when Logic and Accuracy testing is occurring and to program the voting machine to behave correctly during the testing, but to cheat during the election. This is how Volkswagen illegally passed emission tests with cars that were significantly polluting: the cars were programmed to limit the amount of harmful emissions (behave correctly) during the testing, but to allow the harmful emissions (cheat during the election) while driving. The same type of approach could be used with voting machines.
25. County and precinct officials cannot meet their duty to "thoroughly test" the machines because malware potentially loaded on the machines would rarely be detectable in standard testing.
26. County and precinct officials cannot reasonably certify that each machine is working properly because standard testing would not permit officials to determine whether each machine is working properly. Sophisticated malware would likely serve to

- operate the machine properly when it is being tested, and operate in malicious ways during the election.
27. County and precinct officials cannot fulfill their duty to determine whether votes are already recorded in the machine memory card prior to opening of the polls. "Zero tape" print outs can be programmed to print -0- when the machine contains maliciously implanted votes.
 28. If the machines have not been maintained and stored under continuous strict secured physical control prior to and after their use during voting, they are subject to relatively easy entry and manipulation, and must be presumed to be compromised. In such case, local election officials cannot determine whether the machines have been compromised.
 29. The GEMS server, (DRE related equipment), is not secure when flash drives (memory cards) are moved between the GEMS server and internet-connected computers, as is the common practice on Election Night.
 30. The GEMS servers are not secure when databases and memory cards used on the counties' GEMS servers have been exposed to the Internet as they apparently were through the CES server. Such voting system components must be presumed to have compromised the 2017 Special Elections.
 31. Standard testing procedures and routine evaluation of Georgia's voting equipment are inadequate to detect malware in the voting system, or manipulation of results.
 32. Because of the foregoing facts, results of Georgia's recent elections using the DRE-based voting system should not be relied on as accurate, and reflecting the intent of the voters.
 33. Because Georgia's unverifiable voting system was repeatedly exposed to the Internet and other sources of potential intrusion and manipulation, the equipment should be taken out of service immediately.

Further Declarant sayeth not.


Barbara Simons

Curriculum Vitae

Barbara Simons

650.328.8730 voice / 215.243.8002 fax
simons@acm.org

Education

- Ph.D., Computer Science, the University of California, Berkeley, June 1981 - thesis advisor Richard Karp. My dissertation, *Scheduling with Release Times and Deadlines*, solved a major open problem in scheduling theory by developing the first known algorithm for the problem.

Employment

- Co-author with Doug Jones, *Broken Ballots: Will Your Vote Count?*, April 15, 2012.
- Consulting Professor, Stanford University, April 2001 – June 2002; taught courses on Internet technology policy; supervised several students in independent study.
- Retired, IBM, 1998.
- Senior Technology Advisor, IBM Global Services, IBM Corp., Nov. 1996 – 1998; worked with researchers and business people to develop and apply research to business problems.
- Researcher, Application Development Technology Institute, IBM Corp., Oct. 1992 – Nov. 1996; did research on compiler optimization and development of a prototype retargeting compiler backend.
- Research Staff Member, Foundations of Computer Science Group, IBM Research, Jan. 1980 – Sept. 1992; did research on scheduling theory, compiler optimization, fault tolerant distributed computing, and communicating sequential processes.
- Visiting Professor, U.C. Santa Cruz, Sept. 1984 – Dec. 1984; taught graduate algorithms course.

Honors

- Walnut Hills High School Hall of Fame Award, Cincinnati, Ohio, April 30, 2011.
- The Making a Difference Award, Special Interest Group on Computers and Society, 2006.
- Distinguished Alumni Award, College of Engineering, U.C. Berkeley, 2005.
- Computing Research Association's Distinguished Service Award, 2004.
- ACM Outstanding Contribution Award, 2002.
- Distinguished Alumnus Award in Computer Sciences and Engineering, U.C. Berkeley, May 21, 2000.
- Selected as one of the top 25 Women on the Web, 2001, by San Francisco Women on the Web.
- Electronic Frontier Foundation (EFF) Pioneer Award 1998.
- Selected as one of 26 Internet "Visionaries" by c|net, Dec. 1995.
- Selected as one of the Top 100 Women in Computing by Open Computing, Dec. 1994.
- Fellow, ACM, elected 1993.
- Fellow, American Association for the Advancement of Science (AAAS), elected 1993.
- Featured in special issue of *Science* on Women in Science, 1992.
- Computer Professionals for Social Responsibility (CPSR) Norbert Wiener Award for Professional and Social Responsibility in Computing, 1992.
- IBM Research Division Award for work on clock synchronization, 1988.

Policy Interactions with Governmental and Quasi-Governmental Organizations

- Member, Board of Advisors of the federal Election Assistance Commission, appointed by Sen. Harry Reid, August 2008.
- Testified before the Massachusetts legislature in support of voting machine audit legislation, October 22, 2007, Boston, MA.
- Testified before the Committee on House Administration in a hearing on Electronic Voting Machines: Verification, Security, and Paper Trails, September 28, 2006, Washington, DC.
- Member, Security Peer Review Group, a panel of experts who were invited by the U.S. Department of Defense's Federal Voting Assistance Program to evaluate the Secure Electronic Registration and Voting Experiment (SERVE). Co-authored, "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)", with David Jefferson, Aviel Rubin, and David Wagner, released Jan 21, 2004. On Feb. 5, 2004 the Department of Defense announced the cancellation of SERVE because of security concerns.
- Member, Public Interest Registry's .ORG Advisory Council, starting March 2003 – 2006.
- DARPA Panels
 - Member, Information Science and Technology (ISAT) study group on "Security with Privacy", 2002.
 - Member, IPTO workshop on "eDNA: Identification of Origin", Aug. 5-6, 2002.
- Member, National Workshop on Internet Voting, Oct 11-12, 2000, convened at the request of President Clinton. Co-authored with other attendees "Report of the National Workshop on Internet Voting: Issues and Research Agenda", March 2001.
- Runner-up for the North American seat on the Internet Corporation for Assigned Names and Numbers (ICANN) Board, 2000.
- Expert witness, Universal, et al. v. 2600, et al. (the DVD decryption case), July 8, 2000.
- Invited Participant, the White House Conference on the New Economy, Washington, DC, April 6, 2000.
- Member, President's Export Council Subcommittee on Encryption, 1998-2001.
- Member, Information Technology Working Group of the President's Council on the Year 2000 Conversion, 1998 – 2000.
- Testified before Commerce Committee of the California State Senate on encryption, Aug. 26, 1997.
- Testified at hearings before the National Committee on Vital and Health Statistics on privacy issues in the Kennedy-Kassenbaum Bill, San Francisco, CA, June 4, 1997.
- Testified in Social Security Administration hearing: Privacy and Customer Service in the Electronic Age, San Jose State Univ., May 28, 1997.
- Testified in hearing of the Subcommittee of Science, Technology, and Space of the Senate Committee on Commerce, Science, and Transportation on the "Pro-Code" Bill, S.1726, June 26, 1996.
- Testified on Intellectual Property and the Internet before a panel of the Mega-Project III of the Information Infrastructure Task Force (IITF) Advisory Council and the Security Issues Forum of the IITF, Sunnyvale, CA., Oct. 20, 1994.

Boards and Related Activities

- Board of Directors, Verified Voting Foundation, 2004 – present. Currently President.
- Advisory Council, Overseas Vote Foundation's End-to-End Verifiable Internet Voting Project, 2013 – 2015.

- Board of Advisors, ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections), 2008 – 2012.
- Board of Advisors, Electronic Frontier Foundation, 2008 – present.
- Advisory Board, Oxford Internet Institute, Oxford Univ., 2002 – 2006.
- Member, Public Interest Registry's .ORG Advisory Council, 2003 – 2006.
- Board of Directors, Electronic Privacy Information Center, 1998 – 2006. Board Chair, 2005-2006.
- Berkeley Engineering Fund Board of Directors, U.C. Berkeley College of Engineering, 1998 – 2005.
- Advisory Board, Berkeley Foundation for Opportunities in Information Technology, 1999 – present.
- Advisory Board, Public Knowledge, 2001 – 2005.
- Advisory Board, Zeroknowledge Systems Inc., 2000 – 2004.
- Advisory committee, Excellence and Diversity Student Programs, Department of Electrical Engineering and Computer Science, U.C. Berkeley, 1989 – 2004.
- Board of Directors, Math/Science Network, 2002 – 2004.
- Advisory Board, NSF Logging and Monitoring Project (LAMP), Univ. of Michigan, Ann Arbor, Michigan, 2000 - 2002.
- Board of Directors, Council of Scientific Society Presidents, 1998 – 2000.
- Member, steering committee, 21st Century Project, 1995 – 1998.
- Advisory board, the Genome Radio Project and the Telecommunications Radio Project, the Science and Technology Radio Project, 1994 – 95.
- Corporate Affiliates and Advisory Board, Computer Science Division, U.C. Davis, 1991 – 1994.
- Dartmouth Institute for Advanced Graduate Studies, Dartmouth College, 1991 – 1995.
- Member, advisory group, joint ACLU-CPSR projects on a national ID card and privacy, 1989 – 1991.
- Advisory committee, reentry program in computer science, U.C. Berkeley, 1983 - 1989.
- Member, advisory committee at Mills College for the Interdisciplinary Computer Science Program (Masters degree) for returning adults, 1983 - 1986.

Patents

- Retargeting Optimized Code by Matching Tree Patterns in Directed Acyclic Graphs, with Vivek Sarkar and Mauricio Serrano, patent pending.
- A Method of, System for, and Computer Program Product for Providing Efficient Utilization of Memory Hierarchy through Code Restructuring (Patent number 6839895), with Dz Ching Ju, K. Muthukumar, and Shankar Ramaswamy.
- A System, Method, and Program Product for Loop Instruction Scheduling for Hardware Lookahead, with Vivek Sarkar, patent pending.
- A System, Method, and Program Product for Instruction Scheduling in the Presence of Hardware Lookahead Accomplished by the Rescheduling of Idle Slots (Patent number 5887174), with Vivek Sarkar.
- Decentralized Synchronization of Clocks (Patent numbers 4584643 and 4531185), with Danny Dolev, Joe Halpern, and Ray Strong.

Selected Publications

- Voting

- *Broken Ballots: Will Your Vote Count?*, with Doug Jones, Center for the Study of Language and Information, Stanford, CA., June, 2012.
- Report on Election Auditing, by the Election Audits Task Force of the League of Women Voters of the United States, January, 2009.
- Statewide Databases of Registered Voters: Study of Accuracy, Privacy, Usability, Security, and Reliability Issues, co-chaired with Paula Hawthorn, commissioned by ACM's U.S. Public Policy Committee (USACM), February 2006.
- Why Johnny Can't Vote, *APS* (the American Physical Society) *News*, March 8, 2005, p. 8.
- Electronic Voting Systems – the Good, the Bad, and the Stupid, *Queue*, 2, 7, Oct 2004, pp. 20 – 26.
- A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), with David Jefferson, Aviel Rubin, and David Wagner, released Jan 21, 2004. On Feb. 5, 2004 the Department of Defense announced the cancellation of SERVE because of security concerns.
- Report of the National Workshop on Internet Voting: Issues and Research Agenda, with other workshop members, March 2001, sponsored by the National Science Foundation and published by the Internet Policy Institute.

- Other Policy issues
 - Shrink-Wrapping our Rights, Inside Risks, *Commun. ACM* 43, 8, August 2000, p. 168.
 - To DVD or not to DVD, *Commun. ACM* 43, 5, May 2000, pp. 31 – 32.
 - Trademarking the Net, *Commun. ACM* 43, 3, March 2000, pp. 27 – 28.
 - Regulating Content on the Internet, a chapter in *Capital for Our Time*, Hoover Institution Press, Stanford, CA, 1999, pp. 156 – 174.
 - Melissa's Message, *Commun. ACM* 42, 6, June 1999, pp. 25 – 26. Also in *iMP*, an on-line journal.
 - Starr Wars, *Commun. ACM*, Jan. 1999, pp. 26 – 27. Also in *iMP*.
 - Outlawing Technology, *Commun. ACM*, Oct. 1998, pp. 17 – 18. Also in *iMP*.
 - On Building a Research Agenda for Computer Science, *Commun. ACM*, 34, No. 10, Oct. 1991, pp. 121 – 125.

- Scheduling Theory
 - A Fast Algorithm for Multiprocessor Scheduling of Unit-Length Jobs, with Manfred Warmuth, *SIAM J. on Comput.*, 18, No. 4, 1989, pp. 690 – 710.
 - Multiprocessor Scheduling of Unit-Time Jobs with Arbitrary Release Times and Deadlines, *SIAM J. on Comput.*, 12, 1983, pp. 294 – 299.
 - Scheduling Unit-Time Tasks with Arbitrary Release Times and Deadlines, with Michael Garey, David Johnson, and Robert Tarjan, *SIAM J. on Comput.*, 10, 1981, pp. 256 – 269.

- Compiler Optimization
 - A Fast Heuristic for Loop Parallelization, with Richard Anderson, a special issue of *Parallel Processing Letters*, 4(3), 1994, pp. 281 – 299.
 - Parallel Program Graphs and their Classification, with Vivek Sarkar, Proceedings of the 6th Annual Languages and Compilers for Parallelism Workshop, Portland, OR, Aug. 12 – 14, 1993. Springer-Verlag *Lecture Notes in Computer Science*, Vol. 768, Jan. 1994, pp. 633 – 655.
 - Instruction Scheduling for Compilers, with Krishna Palem, IBM Research Report 8535, Dec., 1991. Written to appear as a chapter in *Optimization in Compilers*, edited by Fran Allen, Barry Rosen, and Kenny Zadeck.

- Scheduling Time-Critical Instructions on RISC Machines, with Krishna Palem, *Transactions on Programming Languages (TOPLAS)*, 15, No. 4, 1993, pp. 632 – 658.
- Fault Tolerant Distributed Computing
 - Dynamic Fault-Tolerant Clock Synchronization, with Danny Dolev, Joseph Halpern, and Ray Strong, *Journal of the ACM* 42:1, 1995, pp. 143 – 185.
 - *Fault Tolerant Distributed Computing*, coedited with Alfred Spector, Springer-Verlag Lecture Notes in Computer Science, Vol. 448, 1990.
 - A New Look at Fault Tolerant Network Routings, with Danny Dolev, Joseph Halpern, and Ray Strong, *Information and Computation*, 72, 1987, pp. 180 – 196.
- Communicating Sequential Processes
 - Static Analysis of Interprocess Communication, with Peter Ladkin, to appear as a monograph in the Lecture Notes in Computer Science series published by Springer-Verlag.
 - Deadlock Detection for CSP-type Communications, with Peter Ladkin, *Proceedings of the Third International Workshop on Responsive Computer Systems*, Sept. 29 – Oct. 1, 1993, Lincoln, NH, pp. 229 – 239; a chapter in *Responsive Computer Systems: Steps Toward Fault-Tolerant Real-Time Systems*, ed. D. Fussell and M. Malek, Kluwer Academic Pub., 1995.

Invited Talks

- Invited speaker, Mathematical Sciences Research Institute, Berkeley, Ca., Sept. 16, 2015.
- Invited speaker, League of Women Voters, Manhattan, Kansas, September 15, 2013.
- Invited speaker, “Garantias electorales para el Fortalecimiento de la Democracia”, sponsored by the National Registry and Minister of the Interior, Bogota, Colombia, May 22, 2013.
- Invited speaker, the CRA-W/CDC (Computing Research Assoc. Comm. on the Status of Women / Coalition to Diversify Computing) Distinguished Lecture Series, Orlando, FL, March 26, 2013.
- TED talk, “Why Can't we Vote Online?”, New York, NY, November 5, 2012.
- Interviewed on Charlie Rose Show, National Public Television, October 4, 2012.
- Distinguished lecture, IBM Research, San Jose, CA., September 12, 2012.
- Invited speaker, Microsoft Research, Redmond, WA, August 8, 2012.
- Keynote, Women in Science and Engineering workshop, Univ. of CA, Berkeley, CA, June 21, 2012.
- EFF “Geek Reading”, San Francisco, CA., May 29, 2012.
- Invited speaker, “The Electoral Code that Colombia Needs”, sponsored by the United Nations Development Programme, Bogota Colombia, March 1, 2012.
- Invited by the Mayor of Tallinn, Estonia on a fact finding mission of their Internet voting system, July 18 -19, 2011, Tallinn, Estonia.
- Invited speaker, Workshop on e-voting, European Parliament, March 17, 2011, Brussels.
- Speaker, panel on Internet Voting, Internet, Politics, Policy 2010: An Impact Assessment, Oxford Internet Institute, Oxford, UK.
- Invited by U.S. Department of State's Bureau of International Information Program to speak on voting technology to representatives of government of Bahrain, March 24, 2010, Seattle, WA.
- Keynote speaker, annual conference of The Consortium for Computing Sciences in Colleges Northwest Region, Ashland, OR, October 10, 2008.
- Speaker, Distinguished Lecture Series, the University of Oregon, Eugene, OR, March 13, 2008.
- Invited speaker, Google, Mountain View, CA., December 7, 2007.

- Speaker, National Institute on Computing and the Law, sponsored by the American Bar Association, San Francisco, CA, June 25 – 26, 2007.
- Speaker, Distinguished Speaker Series, U.C. Santa Cruz, Santa Cruz, CA, March 14, 2007.
- Blair O. and Teresa A. Rieth Lecturer, DePauw University, Greencastle, Indiana, November 1, 2006.
- Speaker, Symposium on 21st Century Copyright Law in the Digital Domain, University of Michigan, Ann Arbor, MI, March 24, 2006.
- Keynote speaker, 10th European Symposium on Research in Computer Security (ESORICS 2005), Milan, Italy, September 12, 2005.
- Speaker, Distinguished Lecture Series on Computation and Society, Harvard Univ., Dec. 16, 2004.
- Speaker, 2004 Industrial Physics Forum of the American Physical Society, IBM Research, Yorktown, NY, Oct 25, 2004.
- Speaker, Gordon Research Conference on Science & Technology, Big Sky, MT., Aug. 16, 2004.
- Plenary speaker, 25th Anniversary Celebration, Informatics Division, Universitaet Bremen, Bremen, Germany, Oct. 10, 2003.
- Speaker, 2003 Financial Markets Conference – Business Method Patents and Financial Services, sponsored by the Federal Reserve Bank of Atlanta, Sea Island, GA., April 2-5, 2003.
- Speaker, The Public Voice in the Digital Economy Conference, in conjunction with the OECD-APEC Global Forum: Policy Frameworks for the Digital Economy, Honolulu, HI, Jan 14, 2003.
- Plenary speaker, International Symposium on Computer and Information Sciences, Orlando, FL, Oct 28-30, 2002.
- Keynote, IT Career Events for Indiana Women, Oct. 22, 2002.
- Plenary session, *Castig a Wider Net: Integrating research and policy on the social impacts of the Internet*, conference inaugurating the Oxford Internet Institute, Oxford, England, Sept. 27, 2002.
- Plenary speaker, Management of Digital Rights, Germany, Nov. 20 – 21, 2000.
- Speaker, World Knowledge Forum, South Korea, Oct. 18 – 19, 2000.
- Keynote Panelist, Grace Hopper Conf. on the Future of Computing, Sept 16, 2000, Cape Cod, MA.
- Keynote, S. Africa, SAICSIT'99 (The South African Institute for Computer Scientists and Information Technologists), Johannesburg, South Africa, Nov. 17 – 19, 1999.
- Other talks on computerized voting
 - Panelist, Voter Registration Databases, Electronic Verification Network Conference, San Diego, CA, March 6, 2014.
 - League of Women Voters, California Convention, May 18, 2013.
 - Mills College, April 11, 2013.
 - Distinguished lecture: Clemson Univ., Wofford College, Furman College, Winthrop, Univ., (South Carolina), and Univ. of Iowa, Iowa City, Iowa, Feb. 17 – 22, 2013.
 - Panelist, EVT/WOTE conference, Bellvue, WA, August 7, 2012.
 - “Voice of the Voters!”, Philadelphia, PA (and the internet), April 30, 2008.
 - Tufts University, Boston, MA, October 24, 2007.
 - Boston University, Boston, MA, October 23, 2007.
 - *E-voting*, panelist, 1st Annual National Institute on Computing and The Law, sponsored by the American Bar Association, San Francisco, CA, June 25- 26, 2007.

- Plenary session, *Electronic Voting Integrity*, Computers, Freedom, and Privacy Conference, Montreal, Canada, May 4, 2007.
- *Are We a Democracy? Vote-Counting in the US*, panelist at AAAS Annual Meeting, San Francisco, CA, February 16, 2007.
- *Voting Databases*, panelist at Computers, Freedom, and Privacy Conference, Washington, DC, May 4, 2006.
- University of California at Davis, Davis, CA, March 3, 2005.
- University of Virginia Law School, Charlottesville, VA, February 6, 2005.
- University of Michigan, Ann Arbor, MI, Oct. 5, 2004.
- Center for Discrete Mathematics and Theoretical Computer Science, Rutgers Univ., Piscataway, NJ, May 26-27, 2004.
- San Francisco School of Law, San Francisco, CA., April 21, 2004.
- Oxford Internet Institute, Oxford, England, March 19, 2004.
- Cambridge University, Cambridge, England, March 18, 2004.
- Speaker, Claim Democracy Conference, Nov. 22-23, 2003, Washington, DC.
- Stanford Law School, Stanford, CA., Oct. 30, 2003.
- Panelist, Judge A. Leon Higginbotham Memorial Voting Rights Braintrust panel on voting, sponsored by the Congressional Black Caucus, Washington DC, Sept. 26, 2003.
- Intellectual Property and the Net
 - 21st Century Copyright Law in the Digital Domain, Michigan Telecommunications and Technology Law Review Journal sponsored conference, University of Michigan, Ann Arbor, MI, March 24, 2006.
 - SIGGRAPH 2003. San Diego, July 28, 2003.
 - Harvey Mudd College, Dec. 5, 2002.
 - Distinguished Women Lecture Series, Univ. of Maryland, April 10, 2002.
 - National Institute of Standards and Technology (NIST), Feb. 8, 2002.
 - DIMACS Workshop on Management of Digital Intellectual Prop., Rutgers Univ., April 17 – 18, 2000.
 - ABA National Convention, Aug. 8, 1999.
 - Plenary speaker, ACM Special Interest Group on Computer-Human Interaction, May 19, 1999
 - Distinguished Lecture Series, Brown Univ., Feb. 14, 1999.
 - “Intellectual Capital: Business Strategies, Legal Protections, and Global Competitiveness”, Hoover Institution (Stanford), June 19, 1997.
 - Univ. of Maryland Distinguished Lecture Series, May 1, 1996.
 - Invited Conference Chair and speaker, Intellectual Property, Patent and Copyright Protection on the Internet, Atlanta, GA, April 29, 1996.
- Privacy, Surveillance, and the USA/PATRIOT Act
 - Univ. of Maryland, April 10, 2002.
 - EDUCAUSE National Conference, Indianapolis, IN., Oct. 30, 2001.
 - Richard Tapia Celebration of Diversity in Computing, Houston, Texas, Oct. 20, 2001.
 - Policy Briefing: Emerging Cyberspace Issues Internet Jurisdiction and Global Privacy Protection, the National Press Club, Washington, DC, June 4, 2001
 - Policy Briefing: The Internet, Privacy and the Open Source Movement, the National Press Club, Washington, DC, June 5, 2000.

- “The Future of Public Health: implications for Health Information/Communications Systems,” sponsored by the Ca. Dept of Health Services and the Nat. Centers for Disease Control, San Diego, Ca., March 6, 1996.
- World Affairs Council, San Francisco, CA, April 19, 1994.
- Encryption and Computer Security
 - Plenary session speaker, 9th Annual Conference on Computers, Freedom, and Privacy, Washington, DC, April 1999.
 - “Security and Freedom through Encryption Forum (SAFE),” Stanford Univ., July 1, 1996.
 - Network/Interop Conference, Sept 13, 1994.
 - KPFA radio, Sept. 6, 1994.
 - KQED radio, May 17, 1994.
- National Information Infrastructure
 - DAGS '95 Conference on Electronic Publishing and the Information Superhighway, Boston, MA, June 1, 1995
 - “Issues in Science and Technology Policy,” a Brookings Institute Conference for Corporate and Government Managers, Williamsburg, VA, May 21, 1995.
 - Keynote speaker, Computer Science Conference, Nashville, Tenn., Feb. 28, 1995.
 - National Public Radio’s Science Friday, Feb. 17, 1995.
 - IBM Boulder TechExpo series, Feb. 11, 1995.
 - National Public Radio’s Science Friday, Dec. 10, 1993.

Association for Computing Machinery and Other Professional Society Activities

- Co-Chair, ACM panel on Databases of Registered Voters, 2005 – 2006.
- Founder and Chair or Co-Chair, ACM Technology Policy Committee (USACM), 1993 – 2005.
- Member, Committee to Diversify Computing, 2002 – present.
- Chair, ACM Internet Governance Committee (ACM-IGC), 2000 – 2003.
- Member, ACM-W (ACM’s Committee on Women), 2000 – present.
- ACM President, 1998 – 2000.
- Secretary, Council of Scientific Society Presidents, 1999 – 2000. (Board member 1998 – 2000).
- Member, Computing Research Association (CRA) committee on Public Policy, 1992 – 1996.
- ACM Secretary, 1990 – 1992.
- Member, ACM Committee on Central and Eastern Europe 1990 – 1996.
- Vice-chair, SIGACT (Special Interest Group on Automata and Computability Theory, ACM) 1983 – 1990.
- Member, ACM Government Information Activities Committee, 1989 – 1990.
- Chair, ACM Committee on Scientific Freedom and Human Rights, June, 1987 – 1990.
- Organizer and Chair, SIGACT Science Policy Committee, Nov. 1986 – 1990.

Miscellaneous Professional Activities

- Invited panelist, AAAS Workshop on Developing a Research Agenda for Electronic Voting Machines, Washington, DC, Sept 17 – 18, 2004.
- Runner up for the N. American Seat on the ICANN (Internet Corporation for Assigned Names and Numbers) Board, 2000.
- Women in Science

- Invited participant, National Institutes of Health Summits (Achieving XXcellence '99 and AXXS 2000) on Women in Science, Dec. 9 – 10, 1999 and June 2, 2000.
- Invited participant, National Academy of Engineering Summit on Women in Engineering, May 17 – 18, 1999 and June 2, 2000.
- Invited participant, Women in Science Summit, The Women's Leadership Institute at Mills College, Sept. 29 – Oct. 1, 1994.
- Invited participant, Center for the Advancement of Public Policy multi-media CD-ROM project on Women in the Sciences, March 31, 1994.
- Invited panelist, Forsythe Panel on Women in Computer Science, Stanford Univ., 1986 and 1989.
- Invited participant, Conference on Women and Computers, sponsored by MIT, Nov. 1984, and May 1985.
- Associate Editor, ACM Transactions on the Internet Technology (TOIT).
- Associate Editor, Journal of Computing and Information (JCI).
- Member, the National Science Foundation's Collaboratives for Excellence in Teacher Preparation program review panel, Washington, D.C., Sept. 9 – 11, 1992.
- Member, the National Science Foundation's Research Initiation Awards panel, Washington, D.C., 1989.
- Invited participant, workshop on Science, Engineering and Ethics: State-of-the-Art, sponsored by the AAAS, Feb. 15 – 16, 1988, Boston, MA.
- Member of the National Research Council's Graduate Fellowship Evaluation Panel in Computer Science, Washington, D.C., 1985 – 1987.

EXHIBIT I

March 15, 2017

The Honorable Brian Kemp
214 State Capitol
Atlanta, Georgia 30334

Dear Secretary Kemp,

On March 3rd it was reported that the Federal Bureau of Investigations is conducting a criminal investigation into an alleged cyber attack of the Kennesaw State University Center for Election Systems. According to the KSU Center for Election Systems' website, "the Secretary of State authorized KSU to create a Center for Election Systems, dedicated to assisting with the deployment of the Direct Record Electronic (DRE) voting technology and providing ongoing support."¹ The Center is responsible for ensuring the integrity of the voting systems and developing and implementing security procedures for the election management software installed in all county election offices and voting systems.

The Center has access to most if not all voting systems and software used in Georgia. It also is responsible for programming these systems and accessing and validating the software on these systems. It is our understanding that the Center also programs and populates with voter records the electronic poll books used in polling places statewide. A security breach at the Center could have dire security consequences for the integrity of the technology and all elections carried out in Georgia.

In order for citizens to have faith and confidence in their elections, transparency is crucial, including about events such as the KSU breach, and its extent and severity. While we understand that this investigation is ongoing and that it will take time for the full picture to emerge, we request that you be as forthcoming and transparent as possible regarding critical information about the breach and the investigation, as such leadership not only will be respected in Georgia but also emulated in other states where such a breach could occur. We expect that you are already pursuing questions such as the following, regarding the breach, and trust that you will make public the results of such inquiry:

1. Can you estimate when the attacker breached KSU's system?
2. How did the attacker breach KSU's system?
3. How was the breach discovered?
4. Which files were accessed?
5. Were any files accessed that related to software or "hashes" for the voting machines?
6. Is there any evidence that files were modified? If so, which files?
7. Had KSU begun ballot builds for the upcoming special election?
8. To whom are these attacks being attributed? Could this be an insider attack? Has the FBI identified any suspects or persons of interest?

¹ <http://elections.kennesaw.edu/about/history.php>

9. Has the FBI examined removable media for the possibility of implanted malware?
10. Has the FBI examined the hash or verification program for tampering?
11. What mitigations are planned for the near- and long-term?

In any state an attack on a vendor providing software and system support with such far-reaching responsibilities would be devastating. This situation is especially fragile, because of the reliance on DRE voting machines that do not provide an independent paper record of verified voter intent. KSU has instead sought to verify the validity of the software on the voting machines by running a hash program on all machines before and after elections in an effort to confirm that the software has not been altered. However, if KSU's election programming were compromised, it is also possible that the verification program could have been modified to affirm that the software is correct, even if it were not. This is a risk of using software to check the correctness of software.

Of course all Georgia elections are important. This month and next include special elections as well. If these upcoming elections are to be run on DREs and e-pollbooks that are maintained and programmed by KSU while the KSU Center for Election Systems is itself the subject of an ongoing criminal investigation, it can raise deep concerns. And today's cyber risk climate is not likely to improve any time soon.

We urge you to provide Georgia's citizens with information they need to confirm before going to vote that their name will appear correctly on the voter rolls, as well as back-up printed voter lists in case anomalies appear. Most importantly, we urge you to act with all haste to move Georgia to a system of voter-verified paper ballots and to conduct post-election manual audits of election results going forward to provide integrity and transparency to all of Georgia's elections. We would be strongly supportive of such efforts and would be willing to help in any way we can.

Sincerely,

Dr. Richard DeMillo
Charlotte B. and Roger C. Warren Professor of Computing
Georgia Tech

Dr. Andrew W. Appel
Eugene Higgins Professor of Computer
Science,
Princeton University

Dr. Duncan Buell
Professor, Department of Computer Science
& Engineering, NCR Chair of Computer
Science & Engineering,
University of South Carolina

Dr. Larry Diamond
Senior Fellow, Hoover Institute and
Freeman Spogli Institute, Stanford University

Dr. David L. Dill
Professor of Computer Science,
Stanford University

Dr. Michael Fischer

Dr. J. Alex Halderman

Professor of Computer Science,
Yale University

Professor, Computer Science and Engineering
Director, Center for Computer Security and
Society
University of Michigan

Dr. Joseph Lorenzo Hall
Chief Technologist,
Center for Democracy & Technology

Candice Hoke
Co-Director, Center for Cybersecurity &
Privacy Protection and Professor of Law,
Cleveland State University

Harri Hursti
Chief Technology Officer and co-founder,
Zyptonite, and founding partner, Nordic
Innovation Labs.

Dr. David Jefferson
Lawrence Livermore National Laboratory

Dr. Douglas W. Jones
Department of Computer Science
University of Iowa

Dr. Joseph Kiniry
Principal Investigator, Galois
Principled CEO and Chief Scientist,
Free & Fair

Dr. Justin Moore
Software Engineer, Google

Dr. Peter G. Neumann
Senior Principal Scientist, SRI International
Computer Science Lab, and moderator of the
ACM Risks Forum

Dr. Ronald L. Rivest
MIT Institute Professor

Dr. John E. Savage
An Wang Professor of Computer Science,
Brown University

Bruce Schneier
Fellow and lecturer
Harvard Kennedy School of Government

Dr. Barbara Simons
IBM Research (retired),
former President Association for Computing
Machinery (ACM)

Dr. Philip Stark
Associate Dean, Division of Mathematics and
Physical Sciences,
University of California, Berkeley

Dr. Vanessa Teague
Department of Computing & Information
systems, University of Melbourne

Affiliations are for identification purposes only, they do not imply institutional endorsements.

EXHIBIT J

May 24, 2017

The Honorable Brian Kemp
214 State Capitol
Atlanta, Georgia 30334

Dear Secretary Kemp,

On March 14th we sent a letter to you expressing grave concerns regarding the security of Georgia's voting systems and requesting transparency from your office concerning key questions about the reported breach at Kennesaw State University Center for Election Systems (KSU).

The FBI has reportedly closed its investigation into the breach at KSU and will not be pressing federal charges¹ but regrettably little more is known. We remain profoundly concerned about the security of Georgia's votes and the continued reliance on Diebold paperless touchscreen voting machines for upcoming elections.²

The FBI's decision not to press charges should not be mistaken for a confirmation that the voting systems are secure. The FBI's responsibility is to investigate and determine if evidence exists indicating that federal laws were broken. Just because the FBI concluded this hacker did not cross that line does not mean that any number of other, more sophisticated attackers could not or did not exploit the same vulnerability to plant malicious software that could be activated on command. Moreover, the FBI's statement should not be misinterpreted to conclude that KSU or the Georgia voting system do not have other security vulnerabilities that could be exploited by malicious actors to manipulate votes.

Any breach at KSU's Election Center must be treated as a national security issue with all seriousness and intensity. We urge you to engage the Department of Homeland Security and the US Computer Emergency Readiness Team (CERT) to conduct a full forensic investigation. We cannot ignore the very real possibility that foreign actors may be targeting our election infrastructure.

The FBI investigation lasted a mere few weeks. It's our understanding that this investigation was designed to determine whether criminal charges should be brought. However, a truly comprehensive, thorough and meaningful forensic computer security investigation likely would not be completed in just a few weeks, and it could take many months to know the extent of all vulnerabilities at KSU, if any have been exploited and if those exploits extended to the voting systems. Time and again cyber breaches are found to have been far more extensive than initially reported. When the breach at the Office of Personnel and Management was discovered in March of 2014 it was not disclosed to the public because officials concluded (incorrectly) that there was no loss of personal identifying information. The system was then reviewed by a private security

¹ Torres, Kristina, "Feds: "Security Researcher" behind KSU data breach broke no federal law," *Atlanta Journal Constitution*, March 31, 2017

² Diamont, Aaron, "KSU takes back seat in Georgia elections after server hack," *WSB-TV2 Atlanta News*, March 17, 2017

firm which determined in May (again incorrectly) that the system's security was sound.³ One month later news reports surface warning that 25,000 individuals' personnel records have been compromised. A year later, that number had grown to over 21 million plus the fingerprints of 5.6 million employees.⁴

Problems reported during the April 18th special election have only escalated our concerns. According to news reports, an error occurred during the uploading of votes in Fulton County on election night.⁵ Fulton's director of registration and elections, claimed that when a memory card was uploaded to transfer vote totals the operation failed and the system generated an error message that was "gobbledygook, just junk, just letters."⁶ This sort of error message could be the result of a corrupted database and more investigation is needed.

While one cause of database corruption could be cyber intrusion which should not be ruled out, it is important to note that it was documented over ten years ago that the Diebold GEMS database used in Georgia is vulnerable to database corruption, especially if databases are run concurrently⁷ as reportedly occurred in the recent special election.⁸ This is because GEMS was built on Microsoft JETS database software, an outdated database which cannot be relied upon to provide accurate data.

According to Microsoft:

*"When Microsoft JETS is used in a multi-user environment, multiple client processes are using file read, write, and locking operations on a shared database. Because multiple client processes are reading and writing to the same database and because JETS does not use a transaction log (as do the more advanced database systems, such as SQL Server), it is **not possible to reliably prevent any and all database corruption.**"*⁹[Emphasis added.]

The voting system database stores the vote data. Corruption of the database could mean vote data, or vote counts, are lost. Because Georgia still relies on touchscreen voting machines that do not provide a paper ballot, if votes data is corrupted, it is possible that vote totals could be lost and without a physical paper ballot, there is no way to restore and correct the vote count.

This would be an excellent time to move with all expediency to replace Georgia's outdated voting system, to adopt paper ballot voting and implement robust manual post-election audits. The threat that foreign hackers might target the Dutch national elections caused the Netherlands

³ "Timeline: What We Know about the OPM Breach," *NextGov.com*, <http://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/>

⁴ Rosenfeld, Everett, "Office of Personnel and Management: 5.6 million estimated to have fingerprints stolen in breach," *CNBC*, September 23, 2015

⁵ Kass, Arielle, "'Rare error' delays Fulton County vote count in 6th district race," *Atlanta Journal Constitution*, April 19, 2017

⁶ *Ibid.*

⁷ Hoke, Candice, Ryan, Thomas, "GEMS Tabulation Database Design Issues in Relation to Voting System Certification Standards," https://www.usenix.org/legacy/event/evt07/tech/full_papers/ryan/ryan.pdf

⁸ Kass, Arielle, "'Rare error' delays Fulton County vote count in 6th district race," *Atlanta Journal Constitution*, April 19, 2017

⁹ How to Troubleshoot and to Repair a Damaged Access 2002 or Later Database, (Rev. 6.1 2006) at <http://support.microsoft.com/default.aspx?scid=kb;en-us;283849>

to cancel all electronic voting and hold its March elections on paper ballots. The U.S. has not responded to the threat of foreign hacking with the same accountability and speed. The former director of U.S. national intelligence James Clapper recently told Congress that foreign hackers will continue to attack and we should expect them in the 2018 and 2020 elections.¹⁰

We believe this is a profoundly serious national security issue. We stand ready to help you any way we can to help protect our democratic process and regain the confidence of voters.

Sincerely,

Dr. Richard DeMillo
Charlotte B. and Roger C. Warren Professor of Computing
Georgia Tech

Dr. Andrew W. Appel
Eugene Higgins Professor of Computer
Science,
Princeton University

Dr. Duncan Buell
Professor, Department of Computer Science
& Engineering, NCR Chair of Computer
Science & Engineering,
University of South Carolina

Dr. David L. Dill
Professor of Computer Science,
Stanford University

Dr. Michael Fischer
Professor of Computer Science,
Yale University

Dr. J. Alex Halderman
Professor, Computer Science and Engineering
Director, Center for Computer Security and
Society
University of Michigan

Candice Hoke
Co-Director, Center for Cybersecurity &
Privacy Protection and Professor of Law,
Cleveland State University

Harri Hursti
Chief Technology Officer and co-founder,
Zyptonite, and founding partner, Nordic
Innovation Labs.

Dr. David Jefferson
Lawrence Livermore National Laboratory

Dr. Douglas W. Jones
Department of Computer Science
University of Iowa

Dr. Joseph Kiniry
Principal Investigator, Galois
Principled CEO and Chief Scientist,
Free & Fair

¹⁰ Ng, Alfred, "Ex-intel chief James Clapper warns of more Russian hacks," *CNET*, May 8, 2017

Dr. Ronald L. Rivest
MIT Institute Professor

Dr. John E. Savage
An Wang Professor of Computer Science,
Brown University

Dr. Barbara Simons
IBM Research (retired),
former President Association for Computing
Machinery (ACM)

Dr. Philip Stark
Associate Dean, Division of Mathematics and
Physical Sciences,
University of California, Berkeley

Dr. Vanessa Teague
Department of Computing & Information systems,
University of Melbourne

Affiliations are for identification purposes only, they do not imply institutional endorsements.

EXHIBIT K



OFFICE OF SECRETARY OF STATE

I, Karen C. Handel, Secretary of State of the State of Georgia, do hereby certify that

The AccuVote TS R6 and the AccuVote TSX Voting System, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS firmware version 1.94w, Encoder software version 1.32, Key Card Tool 1.01, ExpressPoll 4000 and ExpressPoll 5000 firmware version 2.1.2 with card writer 1.1.4.0, manufactured by Premier Election Solutions, Inc. formerly known as Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Chapter 2 of Title 21 of the Official Code of Georgia; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to ensure that it continues to be one that can be safely used by the voters of this state. ~~~~~

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 8th day of May, in the year of our Lord Two Thousand and Eight and of the Independence of the United States of America the Two Hundred and Thirty-Second.



Karen C. Handel

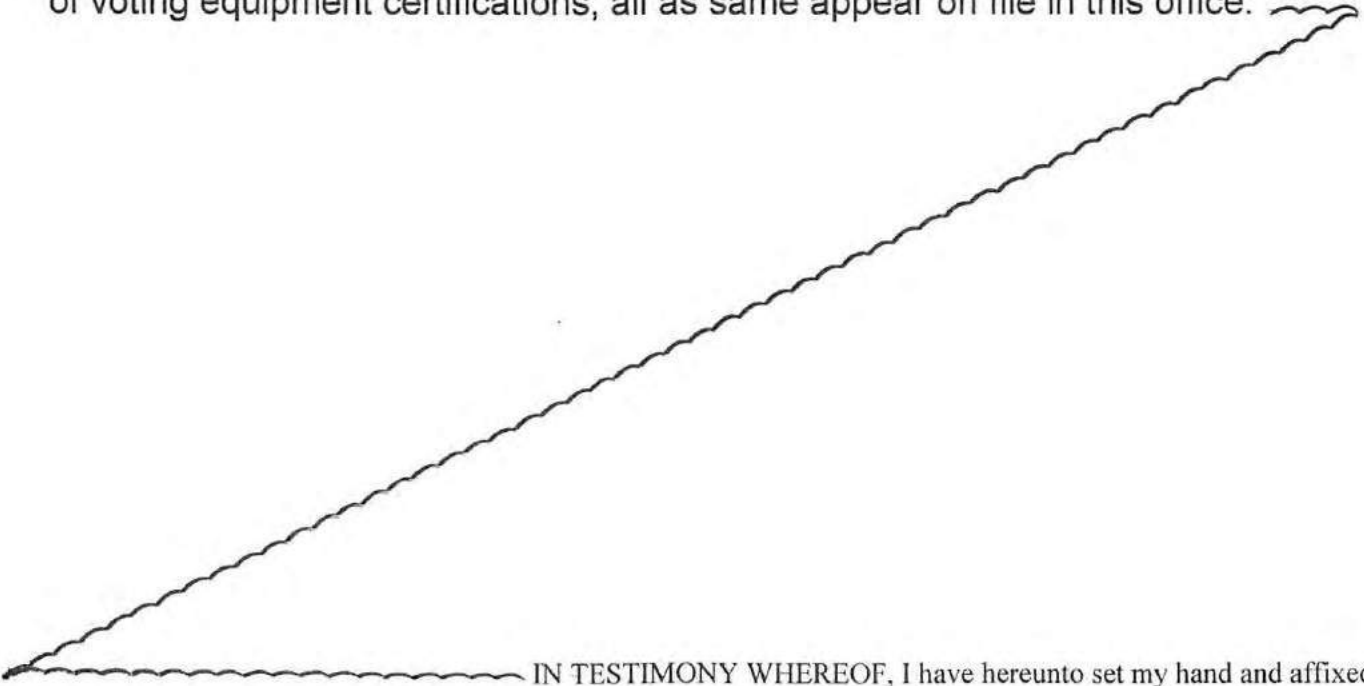
Karen C. Handel, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Karen C. Handel, Secretary of State of the State of Georgia, do
hereby certify that*

the attached nine pages, labeled A through I, are true and correct copies
of voting equipment certifications; all as same appear on file in this office.

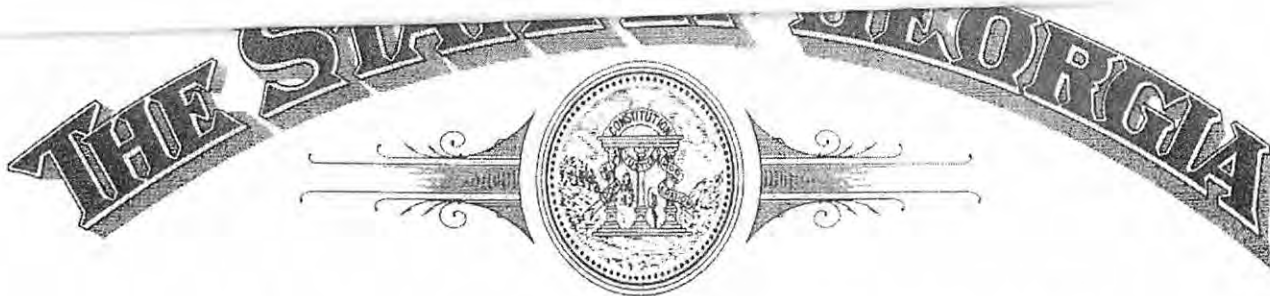


IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed
the seal of my office, at the Capitol, in the City of Atlanta,
this 18th day of April, in the year of our Lord Two
Thousand and Eight and of the Independence of the United
States of America the Two Hundred and Thirty-Second.



Karen C Handel

Karen C. Handel, Secretary of State



OFFICE OF SECRETARY OF STATE

I, Karen C. Handel, Secretary of State of the State of Georgia, do hereby certify that

the attached one (1) page constitutes a true and correct copy of the certification of the AccuVote TS R6 Voting System, consisting of GEMS Version 1.1822G, AVTS firmware version 4.5.2, AVOS firmware version 1.94W, Encoder software 1.3.2, and Key Card Tools 1.0.1, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, for use by the electors of the State of Georgia in all primaries and elections as provided in Georgia Election Code 21-2; all as same appear on file in this office.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 27th day of November, in the year of our Lord Two Thousand and Seven and of the Independence of the United States of America the Two Hundred and Thirty-Second.



Karen C Handel

Karen C. Handel, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

The AccuVote TS R6 and the AccuVote TSX Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 10th day of July, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirty-First.



Cathy Cox

Cathy Cox, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

For the purposes of a Conditional Interim Certification the AccuVote TS R6 and the AccuVote TSX Voting System, consisting of GEMS version 1.18.24, AVTS firmware version 4.6.4, and AVTS voting stations with the attached AccuView Printer Module (The following components of the Georgia voting system were included in the test to verify compatibility: GEMS 1.18.22G, AccuVote TS R6 voting stations with firmware AVTS 4.5.2, AccuVote TSX voting stations with AccuVote firmware AVTS 4.5.2, and ExpressPoll 4000 1.2.0.), manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; the Conditional Interim Certification shall expire on December 31, 2006.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 9th day of August, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirty-First.



Cathy Cox, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

The AccuVote TS R6 and the AccuVote TSX Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 14th day of April, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirtieth.



Cathy Cox, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

The AccuVote TS R6 Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 20th day of September, in the year of our Lord Two Thousand and Five and of the Independence of the United States of America the Two Hundred and Thirtieth.



Cathy Cox

Cathy Cox, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

The AccuVote TS R6 Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 20th day of September, in the year of our Lord Two Thousand and Five and of the Independence of the United States of America the Two Hundred and Thirtieth.



Cathy Cox

Cathy Cox, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

the AccuVote TS R6 Voting System, consisting of GEMS Version 1.18.22G, AVTS firmware version 4.5.2, AVOS firmware version 1.94W, Encoder software 1.3.2, and Key Card Tools 1.0.1, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.



IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 31st day of December, in the year of our Lord Two Thousand and Four and of the Independence of the United States of America the Two Hundred and Twenty-Ninth.

Cathy Cox

Cathy Cox, Secretary of State



OFFICE OF SECRETARY OF STATE

I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that

the AccuVote TS R6 Voting

System, consisting of GEMS Version 1.18.15, and the AVTS firmware, Version 4.3.14, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 10th day of February, in the year of our Lord Two Thousand and Three and of the Independence of the United States of America the Two Hundred and Twenty-ninth



Cathy Cox

SECRETARY OF STATE



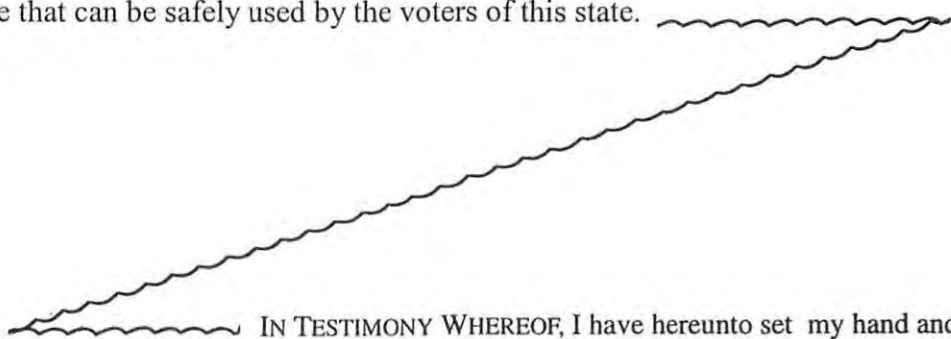
I

OFFICE OF SECRETARY OF STATE

I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that

the AccuVote TS R6 Voting

System, consisting of the AVTS firmware, Version 4.1.11, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.



IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 23th day of May, in the year of our Lord Two Thousand and Two and of the Independence of the United States of America the Two Hundred and Twenty-sixth

Cathy Cox

SECRETARY OF STATE

EXHIBIT L



The Office of Secretary of State

Brian P. Kemp
SECRETARY OF STATE

C. Ryan Germany
GENERAL COUNSEL

June 5, 2017

VIA U.S. MAIL

Mustaque Ahamad
898 Kings Ct NE
Atlanta, GA 30306

David Bader
1824 Charline Ave NE
Atlanta, GA 30306

Ricardo Davis
206 Hunters Mill Lane
Woodstock, GA 30188

Richard DeMillo
2500 Peachtree Rd NW
Unit 606
Atlanta, GA 30305

Virginia Forney
59 Park Lane NE
Atlanta, GA 30309

Merrick Furst
1707 Wildwood Rd NE
Atlanta, GA 30306

Adam Ghetti
606 E. Morningside Drive
Atlanta, GA 30324

Jeff Levy
916 Kings Ct., Unit 1201
Atlanta, GA 30306

Rhonda J. Martin
2500 Peachtree Rd NW
Suite 606
Atlanta, GA 30305

Paul Nally
3667 Hwy 140
Rydal, GA 30171

Michael Opitz
1802 Wynfair Ct.
Marietta, GA 30062

Re: Request for Reexamination of Voting System

Dear Electors,

As the electors who requested a reexamination of the direct recording electronic voting system used throughout Georgia, I wanted to update you on how the Secretary of State's office intends to comply with that request in accordance with O.C.G.A. § 21-2-379.2. Such a request has never been made until now, so I appreciate you bearing with us as we determine the best way to undertake a robust and cost-effective reexamination of the system that includes 27,000 voting machines across the state of Georgia.

Your request differs from requests to review direct recording electronic voting systems prior to being used in Georgia, as the system that you seek to have reexamined has already been deployed statewide. Therefore, a reexamination of that system should be broad enough so that a significant confidence level may be had in the final report. We estimate that such a review will

Letter to Electors
June 5, 2017
Page 2 of 2

cost \$10,000 and will take six months to complete. This estimate is subject to revision as we conduct the reexamination.

You also requested a copy of the most recent certification documentation for the current voting system. Copies of those documents are available for you to review at your convenience at the Office of the Secretary of State, Elections Division, 2 MLK Jr. Dr., Suite 802, West Tower, Atlanta, Georgia, 30334.

Thank you for your interest in Georgia's elections.

Sincerely,



C. Ryan Germany

Cc: Marilyn Marks (marilyn@aspenoffice.com) via email
Dr. Duncan Buell (buell@acm.org) via email

EXHIBIT M

George Balbona

180 Mathews Circle, Marietta, Georgia 30067

Telephone: (404) 641-9632 **Email:** balbonag@mac.com

June 26, 2017

PETITION FOR RECANVASS BY ELECTORS IN THE 6th DISTRICT OF GEORGIA

We, citizens of the 6th District of DeKalb County, Georgia, hereby petition a recanvass of all the memory cards (PCMCIA cards) for the following precincts in DeKalb County:

Briarwood
Ashford Park Elem
Kittredge Elem
Cross Keys High
Mt Vernon West

Recounts and Recanvasses are governed by the Rules of the State Election Board of Georgia, Ga Comp. R. & Regs. 183-1-12-.01:

- (7) Recounts and Recanvass.
 - (a) The election superintendent shall, either of his or her own motion, or upon petition of any candidate or political party or three electors of the county or municipality, as may be the case, order a recanvass of all the memory cards (PCMCIA cards) for a particular precinct or precincts for one or more offices in which it shall appear that a discrepancy or error, although not apparent on the face of the returns, has been made. Such recanvass may be held at any time prior to the certification of the consolidated returns by the election superintendent and shall be conducted under the direction of the election superintendent. Before making such recanvass, the election superintendent shall give notice in writing to each

candidate and to the county chairperson of each party or body affected by the recanvass. Each such candidate may be present in person or by representative and each such political party or body may send two representatives to be present at such recanvass. If upon such recanvass, it shall appear that the original vote count was incorrect, such returns and all papers being prepared by the election superintendent shall be corrected accordingly.

- (b) The election superintendent shall conduct the recanvass by breaking the seal, if the ballots cards have been sealed, on the container containing the memory cards (PCMCIA cards) and removing those memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted. The election superintendent shall then cause the vote totals on each of the memory cards (PCMCIA cards) to be transferred to either an accumulator DRE unit or to the election management system computer. After all of the vote totals from the memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted have been entered, the election superintendent shall cause a printout to be made of the results and shall compare the results to the results previously obtained. If an error is found, the election superintendent shall correct the error in the returns accordingly.

We, three electors of the 6th District in DeKalb County, Georgia, hereby petition for a recanvass of all of the memory cards for the aforementioned precincts because they may contain errors and discrepancies, which must be examined and corrected.

Respectfully submitted,

George Balbona

June 25, 2017

Robert Roche
3633 Chestnut Drive
Doraville, Ga 30340
DeKalb County

I agree with this petition and am happy to contractually and legally bindingly add my signature via this email.

John R. Pastor
3563 Sexton Woods Dr.
Chamblee, Ga.
30341

Ila Dean Fossett

ILA DEAN FOSSETT
1791 HICKORY ROAD
CHAMBLEE, GA 30341

George Balbona

180 Mathews Circle, Marietta, Georgia 30067

Telephone: (404) 641-9632 **Email:** balbonag@mac.com

June 26, 2017

PETITION FOR RECANVASS BY ELECTORS IN THE 6th DISTRICT OF GEORGIA

We, citizens of the 6th District of Cobb County, Georgia, hereby petition a recanvass of all the memory cards (PCMCIA cards) for the following precincts in Cobb County:

Chattahoochee 01
Marietta 5A
Marietta 6A
Marietta 6B
Marietta 7A
Powers Ferry 01

Bells Ferry 03
Roswell 01
Mount Bethel 01
Hightower 01
Eastside 02
Murdock 01

Eastside 01
Fullers Park 01

Recounts and Recanvasses are governed by the Rules of the State Election Board of Georgia, Ga Comp. R. & Regs. 183-1-12-.01:

(7) Recounts and Recanvass.

- (a) The election superintendent shall, either of his or her own motion, or upon petition of any candidate or political party or three electors of the county or municipality, as may be the case, order a recanvass of all the memory cards (PCMCIA cards) for a particular precinct or precincts for one or more offices in which it shall appear that a discrepancy or error, although not apparent on the face of the returns, has been made. Such recanvass may be held at any time prior to the certification of the consolidated returns by the election superintendent and shall be conducted under the direction of the election superintendent. Before making such recanvass, the

election superintendent shall give notice in writing to each candidate and to the county chairperson of each party or body affected by the recanvass. Each such candidate may be present in person or by representative and each such political party or body may send two representatives to be present at such recanvass. If upon such recanvass, it shall appear that the original vote count was incorrect, such returns and all papers being prepared by the election superintendent shall be corrected accordingly.

- (b) The election superintendent shall conduct the recanvass by breaking the seal, if the ballots cards have been sealed, on the container containing the memory cards (PCMCIA cards) and removing those memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted. The election superintendent shall then cause the vote totals on each of the memory cards (PCMCIA cards) to be transferred to either an accumulator DRE unit or to the election management system computer. After all of the vote totals from the memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted have been entered, the election superintendent shall cause a printout to be made of the results and shall compare the results to the results previously obtained. If an error is found, the election superintendent shall correct the error in the returns accordingly.

We, three electors of the 6th District in Cobb County, Georgia, hereby petition for a recanvass of all of the memory cards for the aforementioned precincts because they may contain errors and discrepancies, which must be examined and corrected.

Respectfully submitted,



George Balbona

George Balbona

George Balbona

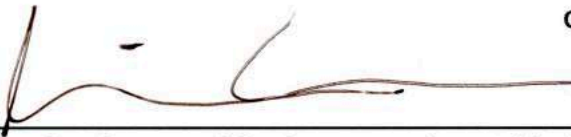


ALLISON KNOCH
NOTARY PUBLIC
GWINNETT COUNTY, GEORGIA
MY COMMISSION EXPIRES
DECEMBER 21, 2017

Sworn to and submitted before me this 25th day of June, 2017.

Cathy Balbona

Cathy Balbona



ALLISON KNOCH
NOTARY PUBLIC
GWINNETT COUNTY, GEORGIA
MY COMMISSION EXPIRES
DECEMBER 21, 2017

Sworn to and submitted before me this 25th day of June, 2017.



Brian Peters



ALLISON KNOCH
NOTARY PUBLIC
GWINNETT COUNTY, GEORGIA
MY COMMISSION EXPIRES
DECEMBER 21, 2017

Sworn to and submitted before me this 25th day of June, 2017.

EXHIBIT N

Rocky Mountain Foundation

7035 Marching Duck Drive E504

Charlotte, NC 28210

704 552 1518

Marilyn@RockyMountainFoundation.org

June 24, 2017

Fulton County Board of Elections

Hand delivered

(Also via email felisa.cordy@fultoncountyga.gov

richard.barron@fultoncountyga.gov

Dwight.Brower@fultoncountyga.gov)

Dear Fulton County Board of Elections:

As you consider the certification of the 6th Congressional District special election, we respectfully request that you decline to certify the June 20 election results. Rocky Mountain Foundation is a non-profit, non-partisan organization focused on election integrity, and makes this request on behalf of our members who were voters in the June 20 election.

Significant security lapses and system intrusions are known to have plagued the voting system in the months leading up the election. Fulton County election officials have not taken responsible forensic measures to analyze whether the system was safe for use, and in fact, has irresponsibly and repeatedly ignored experts' warnings that the system cannot be considered secure or accurate for the conduct of the June 20 election.

The current situation is analogous to a paper ballot election conducted using an unsecured ballot box left open for the entire election with only sporadic oversight. This board would be unable to certify the results of such a paper ballot election because of the security failure of chain of custody of the ballots. The situation today with voters' electronic ballots is no different. The ongoing significant security failures cannot be overcome to permit a certification of the election.

We urge you not to ratify the improper conduct of the Superintendent and staff by certifying the election where legally required controls were absent, security protections failed, and irregularities in the required protocols exist in numerous areas.

The election results should not be certified for several reasons:

1. For several months, Fulton County officials have been aware of gravely concerning security failures and intrusions, and the lack of even a minimally secured voting system. Officials are and have been aware of expert testimony in

the June 7 Curling v. Kemp et al. hearing that the security lapses render the system insecure and unfit for the conduct of the election. It goes without saying that the security failures have placed the results in considerable doubt, and results should not be certified. The extensive level of the security failures was further exposed in press reports before Election Day of the multiple intrusions into the wide-open CES server.

(<http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255>) Fulton officials ignored the dire warning the reports provided. Such misconduct on the part of officials must not be exacerbated by certifying the returns.

2. On April 18, Fulton County officials exposed the GEMS server and all memory cards to cyber security attack from the Internet by using a common, shared flash drive to upload from the GEMS server to the on-line Clarity ENR system, and then reusing that flash drive in the GEMS server. Such serious lapses in security hygiene must be presumed to have compromised the system, and constitute misconduct on the part of the officials. It cannot be reasonably assumed that the system was safe for vote recording and tabulation, even if this practice had been discontinued on June 20. Exposure to the Internet via shared flash drives undermined the security of the entire election.

Although regulations require direct upload of memory cards to the GEMS server for official results with the stated intent of avoiding cyber-attacks in election night electronic transmission, the poor security hygiene practices in Fulton County only escalate the risk of cyber-attack. The memory cards and the GEMS server were exposed and made vulnerable during the election night electronic transmission and during the physical upload to the GEMS server after the GEMS server was exposed to the Internet through the irresponsible use of shared flash-drives. Such misconduct cannot be ignored by this board.

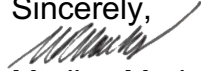
3. The Fulton County collection centers' use of TSx machines to transmit votes from TS machines over modem is not a federally approved standard use of the TSx machine, and not certified to be configured, connected and used in this manner, which exposes the memory cards and GEMS server to cyber-attacks during electronic transmission.
4. The election has been conducted on an illegal voting system that fails to comply with Georgia's election code and related rules. The Secretary of State has not certified the system currently in use as a voting system that can be used "safely and accurately" as required by §21-2-379.2(a). The most recent system certifications by the Secretary of State office have not addressed the safety and accuracy of the systems as require by statute, nor have such certifications covered the current system configuration. Fulton County has chosen to deploy a collection of components that do not meet either the state statutes for an approved voting system or the Secretary of State's regulations for certified voting systems.

5. Physical security of the machines was inadequate prior to the election and during early voting. Given the known exposure of Georgia's system to cyber-attacks and the risk of undetected hacking, it was irresponsible of Fulton County Board and Superintendent to leave machines exposed to easy access by malicious intruders cutting cables and using and replacing tamper-evident seals with identical seals. Although current regulations may permit such risky machine storage in unsecured areas, the board must not irresponsibly rely on permissive and outdated regulations when grave security risks are known to exist. Responsible decisions must be made in light of existing circumstances. If a hallway were flooded with water, machines would not be placed in the water just because the regulations don't prohibit putting machines in flooded areas. Officials have a duty to protect the voting system, and have failed in that duty, in a negligent abuse of discretion.
6. The Board cannot reasonably rely on Logic and Accuracy Testing for any level of assurance of machine accuracy in the wake of the numerous security failures in various areas of the system. As you know, the LAT procedure tests machine operations only in "test mode," and is not a reflection of whether the machine performs accurately in "election mode."
7. On April 18, Fulton County experienced memory card uploading problems to the GEMS server. Officials stated that the GEMS server displayed a message that the upload was successful, with no error messages received until the export of the data from GEMS to the Clarity system. The Superintendent and Board are aware that a functioning, certified GEMS server produces error messages. and does not permit the upload of improper memory cards. This serious problem of no error message signals that the GEMS server is not in safe and proper operational condition, and cannot be relied on to generate accurate election results.
8. The barrage of recent national news with new information on the extent of Russian interference with 2016 elections cannot be ignored given the now proven open access to Georgia's system that existed in 2016 and until at least March 2017. The Board and Superintendent must fulfil their legal duty to conduct a secure election free from the threats of a compromised system.
9. Despite the Superintendent's authority to order a paper ballot election given the known security threats to the DRE system and illegal system configuration, the Superintendent abused his discretion by ignoring multiple expert warnings and conducting the election on a system he knew to be insecure and in violation of laws and regulations. Mr. Barron was present for testimony in the June 7 Curling v. Kemp hearing, and received the pleading including experts' affidavits in that case, and therefore had more than adequate knowledge of the dangers of the uncertified system to require that he employ paper ballots for the proper conduct of the election.

This list is not exhaustive, but provides overwhelming rationale that dictates that a certification of this election cannot be reasonably justified. It supplements the petition for paper ballots delivered to this board on May 11. (attached.)

Thank you for your consideration in this matter. We are happy to provide further documentation of our concerns if it would be helpful to you in your deliberations.

Sincerely,



Marilyn Marks

Executive Director

Rocky Mountain Foundation

Rocky Mountain Foundation
7035 Marching Duck Drive E504
Charlotte, NC 28210
704 552 1518
Marilyn@RockyMountainFoundation.org

June 26, 2017

Director Daniels and DeKalb County Board of Elections
Hand delivered
(Also via email voterreg@dekalbcountyga.gov)

Dear Director Daniels and DeKalb County Board of Elections:

As you consider the certification of the 6th Congressional District special election, we respectfully request that you decline to certify the June 20 election results. Rocky Mountain Foundation is a non-profit, non-partisan organization focused on election integrity, and makes this request on behalf of our members who were eligible voters in the June 20 election.

Significant security lapses and system intrusions are known to have plagued the voting system in the months leading up the election. DeKalb County election officials have not taken responsible forensic measures to analyze whether the system was safe for use, and in fact, has irresponsibly and repeatedly ignored experts' warnings that the system cannot be considered secure or accurate for the conduct of the June 20 election, or the results you plan to certify today.

The current situation is analogous to a paper ballot election conducted using an unsecured ballot box left open for the entire election with only sporadic oversight. This board would be unable to certify the results of such a paper ballot election because of the security failure of chain of custody of the ballots. The situation today with voters' electronic ballots is no different. The ongoing significant security failures cannot be overcome to permit a certification of the election.

We urge you not to ratify the improper conduct by certifying the election where legally required controls were absent, security protections failed, and irregularities in the required protocols exist in numerous areas.

The election results should not be certified for several reasons:

1. For several months, DeKalb County officials have been aware of gravely concerning security failures and intrusions, (particularly those at KSU), and the lack of even a minimally secured voting system. Officials are and have been aware of expert testimony in the June 7 Curling v. Kemp et al. hearing that the security lapses render the system insecure and unfit for the conduct of the

election. It goes without saying that the security failures have placed the results in considerable doubt, and results should not be certified. The extensive level of the security failures was further exposed in press reports before Election Day of the multiple intrusions into the wide-open CES server.

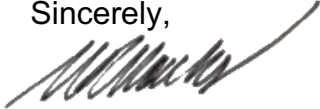
(<http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255>) DeKalb officials ignored the dire warning the reports provided. Such misconduct on the part of officials must not be exacerbated by certifying the returns.

2. The election has been conducted on an illegal voting system that fails to comply with Georgia's election code and related rules. The Secretary of State has not certified the system currently in use as a voting system that can be used "safely and accurately" as required by §21-2-379.2(a). The most recent system certifications by the Secretary of State office have not addressed the safety and accuracy of the systems as require by statute, nor have such certifications covered the current system configuration. DeKalb County has chosen to deploy a collection of components that do not meet either the state statutes for an approved voting system or the Secretary of State's regulations for certified voting systems.
3. The Board cannot reasonably rely on Logic and Accuracy Testing for any level of assurance of machine accuracy in the wake of the numerous security failures in various areas of the system. As you know, the LAT procedure tests machine operations only in "test mode," and is not a reflection of whether the machine performs accurately in "election mode."
4. The barrage of recent national news with new information on the extent of Russian interference with 2016 elections cannot be ignored given the now proven open access to Georgia's system that existed in 2016 and until at least March 2017. The Board and Elections Director must fulfil their duty to conduct a secure election free from the threats of a compromised system.
5. Despite the Board's authority to order a paper ballot election given the known security threats to the DRE system and illegal system configuration, the Director and Board abused their discretion by ignoring multiple expert warnings and conducting the election on a system she knew to be insecure and in violation of laws and regulations. The board was represented by attorneys for testimony in the June 7 Curling v. Kemp hearing, and received the pleadings in that case, and therefore had more than adequate knowledge of the dangers of the uncertified and compromised system to require that Ms. Daniels and the board employ paper ballots for the proper conduct of the election.

This list is not exhaustive, but provides overwhelming rationale that dictates that a certification of this election cannot be reasonably justified.

Thank you for your consideration in this matter. We are happy to provide further documentation of our concerns if it would be helpful to you in your deliberations.

Sincerely,

A handwritten signature in black ink, appearing to read 'M. Marks', with a long, sweeping flourish extending to the right.

Marilyn Marks
Executive Director
Rocky Mountain Foundation

cc: Bennett Bryan (bdbryan@dekalbcountyga.gov)

Rocky Mountain Foundation
7035 Marching Duck Drive E504
Charlotte, NC 28210
704 552 1518
Marilyn@RockyMountainFoundation.org

June 26, 2017

Director Eveler and Cobb County Board of Elections
Hand delivered
(Also via email dwhite@hlclaw.com)

Dear Director Eveler and Cobb County Board of Elections:

As you consider the certification of the 6th Congressional District special election, we respectfully request that you decline to certify the June 20 election results. Rocky Mountain Foundation is a non-profit, non-partisan organization focused on election integrity, and makes this request on behalf of our members who were eligible voters in the June 20 election.

Significant security lapses and system intrusions are known to have plagued the voting system in the months leading up the election. Cobb County election officials have not taken responsible forensic measures to analyze whether the system was safe for use, and in fact, has irresponsibly and repeatedly ignored experts' warnings that the system cannot be considered secure or accurate for the conduct of the June 20 election, or the results you plan to certify today.

The current situation is analogous to a paper ballot election conducted using an unsecured ballot box left open for the entire election with only sporadic oversight. This board would be unable to certify the results of such a paper ballot election because of the security failure of chain of custody of the ballots. The situation today with voters' electronic ballots is no different. The ongoing significant security failures cannot be overcome to permit a certification of the election.

We urge you not to ratify the improper conduct of the Superintendent and staff by certifying the election where legally required controls were absent, security protections failed, and irregularities in the required protocols exist in numerous areas.

The election results should not be certified for several reasons:

1. For several months, Cobb County officials have been aware of gravely concerning security failures and intrusions, and the lack of even a minimally secured voting system. Officials are and have been aware of expert testimony in the June 7 Curling v. Kemp et al. hearing that the security lapses render the

system insecure and unfit for the conduct of the election. It goes without saying that the security failures have placed the results in considerable doubt, and results should not be certified. The extensive level of the security failures was further exposed in press reports before Election Day of the multiple intrusions into the wide-open CES server.

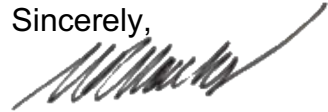
(<http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255>) Cobb officials ignored the dire warning the reports provided. Such misconduct on the part of officials must not be exacerbated by certifying the returns.

2. The election has been conducted on an illegal voting system that fails to comply with Georgia's election code and related rules. The Secretary of State has not certified the system currently in use as a voting system that can be used "safely and accurately" as required by §21-2-379.2(a). The most recent system certifications by the Secretary of State office have not addressed the safety and accuracy of the systems as require by statute, nor have such certifications covered the current system configuration. Cobb County has chosen to deploy a collection of components that do not meet either the state statutes for an approved voting system or the Secretary of State's regulations for certified voting systems.
3. The Board cannot reasonably rely on Logic and Accuracy Testing for any level of assurance of machine accuracy in the wake of the numerous security failures in various areas of the system. As you know, the LAT procedure tests machine operations only in "test mode," and is not a reflection of whether the machine performs accurately in "election mode."
4. The barrage of recent national news with new information on the extent of Russian interference with 2016 elections cannot be ignored given the now proven open access to Georgia's system that existed in 2016 and until at least March 2017. The Board and Elections Director must fulfil their duty to conduct a secure election free from the threats of a compromised system.
5. Despite the Director's authority to order a paper ballot election given the known security threats to the DRE system and illegal system configuration, the Director abused her discretion by ignoring multiple expert warnings and conducting the election on a system she knew to be insecure and in violation of laws and regulations. Ms. Eveler was present for testimony in the June 7 Curling v. Kemp hearing, and received the pleadings in that case, and therefore had more than adequate knowledge of the dangers of the uncertified and compromised system to require that she employ paper ballots for the proper conduct of the election.

This list is not exhaustive, but provides overwhelming rationale that dictates that a certification of this election cannot be reasonably justified.

Thank you for your consideration in this matter. We are happy to provide further documentation of our concerns if it would be helpful to you in your deliberations.

Sincerely,

A handwritten signature in black ink, appearing to read 'M. Marks', with a long, sweeping flourish extending to the right.

Marilyn Marks
Executive Director
Rocky Mountain Foundation

cc: Daniel W. White (dwhite@hlclaw.com)