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

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

COALITION PLAINTIFFS' BRIEF IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

August 3, 2018

Table of Contents

I. INTRODUCTION AND SUMMARY 1
II. LEGAL STANDARDS 2
A. Granting of a Preliminary Injunction 2
B. Procedure and Evidence 2
III. ARGUMENT 3
A. Coalition Plaintiffs Are Likely to Succeed on the Merits 3
1. Georgia's Current DRE System 6
2. DREs Are Profoundly Insecure and Vulnerable 9
3. Georgia's System Has Already Been Compromised 12
4. Secretary Kemp's Agents Have Destroyed All the Evidence of Who Accessed the KSU Server 15
5. Georgia's Voting Security Failure Has Not Been Remedied 16
6. Evidence of Malfunctions in Recent Elections 17
7. International Threat Intensifies: "The Lights Are Blinking" 19
8. Conclusion – Plaintiffs are Likely to Succeed on the Merits 19
B. Plaintiffs Are Likely to Suffer Irreparable Harm 20
C. Balance of Equities Favors Granting the Injunction 22
D. Injunction Is in the Public Interest 25
IV. CONCLUSION 25

Plaintiffs Coalition for Good Governance, William Digges III, Laura Digges, Megan Missett, and Ricardo Davis (the "Coalition Plaintiffs") file this Brief in Support of their Motion for Preliminary Injunction.

I. INTRODUCTION AND SUMMARY

Officials from the highest levels of the Federal Government have issued repeated and increasingly urgent warnings to states like Georgia to *not* use electronic voting machines in the upcoming elections and instead to switch to paper ballots. Defendants stubbornly refuse to take any action, insisting -- against overwhelming evidence to the contrary -- that Georgia's system is secure. The Coalition Plaintiffs are therefore compelled to bring this motion for preliminary injunctive relief to protect their fundamental right to vote and their rights under the Equal Protection Clause of the United States Constitution.

As will be explained below, Georgia AccuVote DRE electronic voting system is extremely vulnerable to undetectable attack or system error. Plaintiffs will further show the likelihood of irreparable harm because the results of any election using the DRE machines is unverifiable and highly likely to be inaccurate. Moreover, notwithstanding the Secretary's protestations to the contrary, Georgia can lawfully switch to a paper ballot system using existing resources with minimal effort. For these reasons, Defendants should be enjoined through the pendency of this litigation from using the unverifiable and hopelessly compromised AccuVote

DRE paperless voting system, and instead should be enjoined to use paper ballots.

II. LEGAL STANDARDS

A. Granting of a Preliminary Injunction

Chief Justice Roberts summarized the familiar test for the granting of a preliminary injunction in *Winter v. NRDC,* 555 U.S. 7, 20 (2008):[1]

> A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest.

These are not rigid requirements to be applied by rote. "The essence of equity jurisdiction has been the power of the Chancellor to do equity and to mold each decree to the necessities of the particular case. Flexibility rather than rigidity has distinguished it." *Weinberger v. Romero–Barcelo,* 456 U.S. 305, 312 (1982).

B. Procedure and Evidence

Though discovery in this case has not formally opened and the Defendants have not answered the Third Amended Complaint, this Motion is not premature. "The grant of a temporary injunction need not await any procedural steps perfecting the pleadings or any other formality attendant upon a full-blown trial of this case." *United States v. Lynd*, 301 F.2d 818, 823 (5th Cir. 1962) (Tuttle, J.).

---

[1] *See also Alabama v. U.S. Army Corps of Engineers*, 424 F.3d 1117, 1131 (11th Cir. 2005).

In considering this Motion, the Court also is permitted to rely upon hearsay and upon affidavits in lieu of live testimony. "[A] preliminary injunction is customarily granted on the basis of procedures that are less formal and evidence that is less complete than in a trial on the merits." *Univ. of Tex. v. Camenisch,* 451 U.S. 390, 395 (1981); *Levi Strauss & Co. v. Sunrise Int'l Trading, Inc.*, 51 F.3d 982, 985 (11th Cir. 1995) (at the "preliminary injunction stage, a district court may rely on affidavits and hearsay materials which would not be admissible evidence for a permanent injunction").

III. ARGUMENT

A. Coalition Plaintiffs Are Likely to Succeed on the Merits

Plaintiffs are likely to succeed on their claims that the use of Georgia's DRE voting system to record votes burdens the Plaintiffs' fundamental right to vote (Count One) and violates the Equal Protection Clause (Count Two).

Plaintiffs' fundamental-right-to-vote claim is based upon "the right of qualified voters within a state to cast their ballots and have them counted." *United States v. Classic,* 313 U.S. 299, 315 (1941). "No right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined." *Wesberry v. Sanders,* 376 U.S. 1, 17 (1964).

This foundational constitutional right necessarily includes the right to have one's vote counted accurately. "Every voter's vote is entitled to be counted once. It must be correctly counted and reported." *Gray v. Sanders,* 372 U.S. 368, 380 (1963). "Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person's vote over that of another." *Bush v. Gore,* 531 U.S. 98, 104-05 (2000).

States may not, by arbitrary action or other unreasonable impairment, burden a citizen's right to vote. *Baker v. Carr,* 369 U.S. 186, 208 (1962) ("citizen's right to a vote free of arbitrary impairment by state action has been judicially recognized as a right secured by the Constitution"). "[T]he free exercise and enjoyment of the rights and privileges guaranteed to the citizens by the Constitution and laws of the United States" entails

> the right and privilege to express by their votes their choice of a candidate for Senator and their right to have their expressions of choice given full value and effect by not having their votes impaired, lessened, diminished, diluted and destroyed by fictitious ballots fraudulently cast and counted, recorded, returned, and certified.

United States v. Saylor, 322 U.S. 385, 386 (1944). *See also Reynolds v. Sims,* 377 U.S. 533, 555 (1964) ("[T]he 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.").

Plaintiffs need not establish at trial, much less at the preliminary injunction stage of the case, that an impairment of their right to have their votes counted accurately has already occurred *or* that it is certain to occur. Instead, Plaintiffs will prevail at trial with a showing that the burden imposed upon their rights by the very substantial risk that votes will be miscounted or diluted by the DRE system outweighs any of the State in insisting upon the continued use of the DRE machines. *Crawford v. Marion County Election Bd.,* 553 U.S. 181, 190 (2008).

As to Plaintiffs' claim under the Equal Protection Clause, the issue is whether Georgia voters using AccuVote DREs are "less likely to cast an effective vote" than absentee voters using paper ballots. *Wexler v. Anderson,* 452 F.3d 1226 (11th Cir. 2006).[2] *See also Dunn v. Blumstein,* 405 U.S. 330, 336 (1972) ("[A] citizen has a constitutionally protected right to participate in elections on an equal basis with other citizens in the jurisdiction.").

There is a substantial likelihood that Plaintiffs will prevail on both claims.

[2] The *Wexler* case involved Florida's use of AccuVote DRE machines, but the plaintiffs there did not allege or prove that the machines were vulnerable to attack. Instead, the plaintiffs' theory was that "by certifying touchscreen voting systems that are incapable of providing for the type of manual recounts contemplated by Florida law, the defendants have violated the equal protection and due process rights of voters in touchscreen counties." 452 F.3d at 1226. In rejecting this claim, the Eleventh Circuit explained that the allegations Plaintiffs make in this case – that voters using touchscreen systems are less likely to cast an effective vote than voters using paper ballots – would state an equal protection violation. *Id.* at 1231.

1. Georgia's Current DRE System

The primary features of Georgia's current DRE system are not in dispute. The voting system used in Georgia today consists of the Diebold Global Election Systems ("Diebold") AccuVote DRE touchscreen voting units ("DREs"), the Diebold optical scanners for tabulating paper ballots, and the Diebold General Election Management Software ("GEMS") for tabulation and reporting of data generated by DRE and Diebold optical scanners, as well as the electronic pollbook components and electronic accessories that interface with the vote recording system. Georgia uses approximately 27,000 Diebold DRE touchscreen voting machines. (Third Amended Complaint ("TAC") ¶ 59).

Each DRE internally contains much of the same hardware that might typically be found in a very low-end general-purpose personal desktop computer in use in the early 2000s. (Bernhard Decl. ¶ 11). Georgia's DREs run a Diebold-modified version of Microsoft's Windows CE operating system, the most recent version run in Georgia is Windows CE 4.1—which Microsoft stopped supporting in early January 2013. (Bernhard Decl. ¶ 11). As a consequence, Microsoft is no longer issuing updates or security patches for that software. (Bernhard Decl. ¶ 23). "As the operating system is over twenty years old, it lags behind the two decades of computer security research and is extremely vulnerable to a wide variety of attacks that Diebold's software, regardless of version, cannot defend against." *Id.*

A proprietary Diebold software application called BallotStation provides the user interface that voters and poll workers see. BallotStation interacts with the voter, accepts, records, and tallies votes on the DRE. (Bernhard Decl. ¶ 21).

DREs are configured by inserting a memory card into a slot behind a locked door on the side of the machine. Before the election, the file system on the memory card stores the election definition, sound files, interpreted code that is used to print reports, and other configuration information. When operating properly, DREs use software to translate the voter's physical act of touching a particular place on the touchscreen into a vote for the corresponding candidate or issue, which vote is then recorded on both the DRE's removable memory card and internal flash memory. Both records of the votes are unreadable to humans. Crucially, Georgia's DREs do not create or retain any non-electronic record of the voter's selections. (Bernhard Decl. ¶ 12; Lamb Decl. ¶ 5).

Upon the closing of the polls, poll workers cause DREs to interpret collected electronic vote information, tabulate vote tallies, and convert it to human readable form to print tallies. The DRE memory cards are removed, secured for transport to a transmission center, in the case of Fulton County, or to county election offices. (TAC ¶ 72-73). DRE memory cards are collected and uploaded into the county election office GEMS server (running on a desktop computer). (TAC ¶ 75).

Georgia uses paper ballots for mail-in absentee ballots and in-person

provisional ballots. These paper ballots are scanned and tabulated by Diebold AccuVote Optical Scan units, located in the county election offices. On election night, the memory cards from the Diebold AccuVote Optical Scan units are uploaded to the Diebold GEMS server and combined with the data from the DREs to create unofficial consolidated results and generate reports in human readable form. (TAC ¶ 76-78).

For present purposes, there are two crucial features of Georgia's election system that must be re-emphasized. First, DREs, by design, create no non-electronic record of voter intent. There is no possible way to verify if the DRE system has correctly recorded and counted the intent of the voters. This is completely unacceptable for public elections. As Director of Homeland Security Kirstjen Nielsen recently testified: "You must have a way to audit and verity the election result."[3] Second – and this is significant in the evaluation of the proposed remedy – every county in Georgia currently uses the paper ballot/optical scan system proposed by Plaintiffs. Thus, the remedy of conducting the upcoming November and December 2018 elections using paper ballots instead of DREs is

[3] Volz, Dustin, and Patricia Zengerle. "Inability to audit U.S. elections a 'national security concern': Homeland chief,"Reuters (March 21, 2018), available at https://www.reuters.com/article/us-usa-trump-russia-security/inability-to-audit-u-selections-a-national-security-concern-homeland-chief-idUSKBN1GX200. For a videotape of Secretary Nielsen's testimony before the Senate, see https://www.youtube.com/watch?v=lXjYNLJ9yAM&feature=youtu.be (video of testimony at 3:38).

eminently feasible.

2. DREs Are Profoundly Insecure and Vulnerable

The unreliability and vulnerability of electronic voting systems like the one used by the State of Georgia has attracted widespread and uniform alarm at all levels of government. On July 26, 2018, House Intelligence Committee Chairman Devin Nunes joined many federal officials and agencies concerned with national security to call for a complete ban on electronic voting.[4] In May, the Senate Select Committee on Intelligence concluded that paperless DREs "are at highest risk of security flaws," and stated that "[s]tates should rapidly replace outdated and vulnerable voting systems" with machines that "[a]t a minimum . . . have a voter-verified paper trail."[5] Similarly, in March, DHS Secretary Nielsen labeled electronic voting systems "a national security concern."[6]

In January 2018, the Congressional Task Force on Election Security issued a Final Report addressing the insecurity of the country's voting infrastructure:

> Given the breadth of security risks facing voting machines, it is especially problematic that approximately 20% of voters are casting their ballots on machines that do not have any paper backup. *These voters are using paperless Direct Recording Electronic (DRE) machines that have been shown over and again to be highly*

[4] http://thehill.com/hilltv/rising/398949-house-intel-chair-calls-for-ban-on-electronic-voting-systems.

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

[6] S*ee supra* note 3.

> *vulnerable to attack.* Because these machines record votes on the internal memory of the machine, and do not leave any paper backup, it is near impossible to detect whether results have been tampered with.[7]

As detailed in the Declaration of Matthew D. Bernhard, attached hereto as Exhibit A, and in the Brief of Amici Curiae Common Cause, National Election Defense Coalition, and Protect Democracy ("Common Cause Amici Brief"), these recent alarms from the federal government amplify years of warnings from computer scientists, who have uniformly concluded that paperless balloting is unreliable, unquestionably insecure, and unverifiable. (Bernhard Decl. ¶¶ 13- 20; Common Cause Amici Brief, [Doc. 240-1, *passim*]). California's 2007 "Top-to-Bottom Review" ("TTBR")[8] found that DREs were "inadequate to ensure accuracy and integrity of the election results…"; that the system contained "serious design flaws that have led directly to specific vulnerabilities, which attackers could exploit to affect election outcomes…"; and that "attacks could be carried out in a manner that is not subject to detection by audit, including review of software logs."[9] Citing these vulnerabilities of the Diebold's AccuVote DREs, California

[7] Congressional Task Force of Election Security, *Final Report*, https://democrats-homeland.house.gov/sites/democrats.homeland.house.gov/files/documents/TFESReport.pdf (Feb. 14, 2018), at 24 (emphasis added).

[8] See Joseph A. Calandrino, et al., *Source Code Review of the Diebold Voting System*, http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf (Jul. 20, 2007).

[9] See California Secretary of State, *Withdrawal Of Approval*, http://votingsystems.cdn.sos.ca.gov/vendors/premier/premier-11824-revision-1209.pdf (Dec. 31, 2009 rev.), at 2, 3.

Secretary of State Debra Bowen decertified California's voting system.[10] Ohio's 2007 "Evaluation and Validation of Election-Related Equipment, Standards and Testing ("EVEREST")[11] concluded that Ohio's AccuVote "system lacks the technical protections necessary to guarantee a trustworthy election under operational conditions." [12]

Any number of published studies are in accord. (Bernhard Decl. ¶¶ 14, 15, 16, 17; *id.,* fn. 1, 2, 3). [13] The vulnerabilities identified by all of these governmental authorities and computer experts apply specifically to the DREs used by the State of Georgia today. (Bernhard Decl. ¶ 21; Lamb Decl. ¶¶ 7-10).

Significantly, the flaws in DREs can be exploited whether or not the machines are directly connected to the Internet. An attacker can gain physical access to a memory card in many different ways and could by that means install malicious code that spreads automatically from machine to machine. Similarly, an attacker could infect the programming by emailing a virus to election officials responsible for programming the machines. An attacker with access to the server on which DRE software is stored – like the KSU server discussed below – could

[10] See *Withdrawal Of Approval*, *supra* note 9, at 5.

[11] Pennsylvania State Univ., et al., *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing*, https://www.eac.gov/assets/1/28/EVEREST.pdf (Dec. 7, 2007).

[12] See *EVEREST*, *supra* note 11, at 103.

[13] *See also* Feldman, et al., "Security Analysis of the Diebold AccuVote-TS Voting Machine," *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop,* 1 (Aug. 2007).

alter the software surreptitiously so that election officials themselves install the malware in the course of election preparations. Demonstrations show that it is easy to break into AccuVote TSXs with nothing more than a BIC pen and install vote-stealing software that changes votes in undetectable ways. (Bernhard Decl. ¶¶ 29-30).

3. Georgia's System Has Already Been Compromised

The already unacceptable extreme vulnerability of Georgia's system was greatly increased by Secretary Kemp's failure to secure the State's central election server before and after the 2016 elections. (*See generally* Lamb Decl. ¶¶ 11- 19). From at least 2002 until at least December 31, 2017, Georgia's Secretaries of State have contracted with Kennesaw State University ("KSU"), for the creation of the Center for Election Services ("CES") at KSU to assist the Secretary in the fulfillment of his statutory duties to manage Georgia's DRE system. CES's Executive Director Merle King maintained a computer server with the URL "elections.kennesaw.edu," on which CES hosted a comprehensive assemblage of electronic files consisting of software applications, password files, tabulation database programs, encryption keys, confidential voter registration information, ballot proofs, technical training videos, and other sensitive information critical to the safe and secure operation of Georgia's DRE-based voting system. The information hosted on the "elections.kennesaw.edu" server was not authorized to

be publicly accessible. But between at least August 2016 and March 2017, and likely for a much longer time, this server was fully accessible to any computer user with Internet access.

In late August 2016, cybersecurity researcher Logan Lamb accessed files hosted on the "elections.kennesaw.edu" server on the public internet, including the voter histories and personal information of *all* Georgia voters, tabulation and memory card programming databases for past and future elections, instructions and passwords for voting equipment administration, and executable programs controlling essential election resources. When he accessed these sensitive files, Lamb noted that the files had been publicly exposed for so long that Google had cached (i.e., saved digital backup copies of) and published much of the sensitive data on the Internet. (Lamb Decl. ¶¶ 13- 14).

On August 28, 2016, Lamb contacted King by telephone and email to warn him that CES should assume that the sensitive documents hosted on the "elections.kennesaw.edu" server had already been downloaded by unauthorized persons and that all sensitive files should be considered compromised. King immediately informed CES staff of the breach. Yet for reasons that have never been explained, the server was not secured for months. Lamb and colleague Christopher Grayson accessed the server again several times in late February 2017 and on March 1, 2017, and they were repeatedly able to access and download the

same types of files that Lamb had accessed months earlier. (Lamb Decl. ¶ 15).

On March 1, 2017, Grayson contacted a KSU Computer Science Instructor and informed him of the exact times and IP addresses of his own recent repeated access of the unsecured voting system server. KSU finally caused the elections server to be isolated from the public Internet on or about March 1, 2017.

After it became known that the "elections.kennesaw.edu" server was compromised, CES staff emails indicate that Secretary Kemp's agents at KSU did not conduct or order a forensic examination to determine whether the server had been altered or manipulated. Neither Secretary Kemp's agents at KSU, nor his internal staff at the Secretary of State's office, has ever properly verified the integrity of any software, passwords, databases or encryption keys that were hosted on the compromised "elections.kennesaw.edu" server. As a consequence, the compromised software, passwords, and encryption keys *continue to be used* on the equipment that has been and will be employed to conduct Georgia's public elections. (Lamb Decl. ¶ 19).

According to recent indictments issued by Special Counsel Robert Mueller, at the same time that Lamb was alerting Secretary Kemp's team at KSU that Georgia's server was completely exposed, and Secretary Kemp's team were doing nothing about it, Russian operatives were visiting "the websites of certain counties

in Georgia, Iowa, and Florida to identify vulnerabilities."[14]

4. Secretary Kemp's Agents Have Destroyed the Evidence of Who Accessed the KSU Server

Evidence of these and other intrusions into Georgia's system has probably been destroyed and lost forever due to the deliberate actions of Secretary Kemp's agents after the filing of this lawsuit. At least by the filing of this lawsuit on July 3, 2017, Secretary Kemp and his agents were under a duty to preserve evidence. In clear breach of this duty, the Secretary's agents, three days after this lawsuit was filed, destroyed all data on the hard drives of the KSU "elections.kennesaw.edu" server. On August 9, 2017, less than 24 hours after this action was removed to this Court, Secretary Kemp's agents went further and destroyed all data on the hard drives of a secondary server hosted at "unicoi.kennesaw.edu," which contained similar, but not identical data, to that on the "elections.kennesaw.edu" server. The "logfiles" that contain historical records of external access from the public Internet to the "elections.kennesaw.edu" and "unicoi.kennesaw.edu" servers would have been deleted when all data on the respective servers' hard drives were destroyed.

The destruction of this data is significant in two respects. First, the loss of the data will make it impossible for Georgia to determine the nature and extent of any intrusions into the system and, accordingly, to remedy the harm caused

[14] *United States v.Netyksho, et al.,* Indictment (D.D.C., July 13, 2018) ¶ 75.

thereby. Second, the destruction of the data on these servers entitles Plaintiffs, at a bare minimum, to evidentiary presumptions that will make success on the merits even more likely. *Kraft Reinsurance Ireland, Ltd. v. Pallets Acquisitions, LLC*, 845 F. Supp. 2d 1342, 1358 (N.D. Ga. 2011) ("Spoliation is the destruction...of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.").

5. Georgia's Voting Security Failure Has Not Been Remedied

Secretary Kemp may contend that the fact that Georgia's server may have been ravaged by foreign or domestic criminals in 2016 and 2017 does not have an impact on the current vulnerability of Georgia's election system because election files are now on a new server with purported proper security under the direct control of the Secretary of State.

The overwhelming evidence, however, establishes to the contrary. "A massive, time-consuming effort would be required to address the security breaches that occurred in Georgia," states expert Matt Bernhard, "requiring experienced technicians to give hands-on attention to individual machines (tens of thousands of pieces of equipment), one at a time." (Bernhard Decl. ¶ 44). Because of the interconnected nature of the system, which consists of thousands of vulnerable electronic components, properly decontaminating the components at risk across the state would be a nearly impossible undertaking. (Bernhard Decl. ¶ 45; *see also*

Lamb Decl. ¶ 20). There is no evidence that Georgia has even attempted to mitigate the massive risks created by the KSU exposure.

6. Evidence of Malfunctions in Recent Elections

In addition, there is alarming new evidence that Georgia's DRE voting system has inexplicably malfunctioned in recent elections in ways that impact voters directly:

- Voter eligibility information in the Diebold electronic pollbooks (part of the certified DRE system) differs from Secretary of State's official voter registration records, which has caused potential and actual disenfranchisement. (Clark Decl. ¶¶ 10-15; Bowers Decl. ¶¶ 35-46; Marks Decl. ¶ 2).
- Inaccurate political party designation in electronic pollbook has caused voter disenfranchisement. (Luse Decl. ¶¶ 6-8).
- Unauthorized changes in the voter registration records have changed polling places and assigned voters to improper districts. (Mitchell Decl. ¶¶ 8-11).
- Inaccurate DRE electronic ballots have been issued to at least one voter, causing the DRE screen to display wrong districts and candidates during early voting – plainly subjecting unwary voters to disenfranchisement. (Kadel Decl. ¶¶ 8-28).

- Numerous polling place recap sheets provided by Fulton County to Coalition Plaintiffs have revealed unresolved material differences between the number of voters voting at the polling place and the number of ballots cast as reported on the DRE machine results tapes. (Marks Decl. ¶ 2, Ex. 2).
- A DRE machine tabulation results tape in Hall County did not include results from 9 races, suggesting the possibility that voters were not given a complete ballot or votes were not counted. (Bowers Decl. ¶¶ 5-8; Copeland Decl. ¶ 5).
- DRE machines have printed irregular timestamps indicating materially delayed ballot tallies and reporting and machine malfunction. (*E.g.,* Bowers Decl. ¶ 19; Copeland Decl. ¶ 9).
- A Hall County voting machine malfunctioned, was taken out of service and showed no votes cast on a delayed closing tape. Pollworkers had difficulty closing the polls and disagreed on whether votes were cast on the problem machine. (Bowers Decl. ¶¶ 25-31).
- Voter turnout of more than 100% was reported in precincts in Habersham County and Fulton County. (Marks Decl. ¶ 4, Ex. 3).

It is almost a certainty that the discrepancies reported to Plaintiffs and described above are only a small fraction of the actual number of problems encountered state-wide. These errors are consistent with the kinds of errors that

experts would expect to be generated by malware, programming errors, or other sources of computer system malfunction. (Bernhard Decl. ¶ 49).

7. International Threat Intensifies: "The Lights Are Blinking"

The vulnerability of Georgia's DRE voting system is not only an issue of past exposure, but a matter of ongoing and growing concern. Director of National Intelligence Daniel Coats stated on July 17, 2018: "Every day, foreign actors — the worst offenders being Russia, China, Iran and North Korea — are penetrating our digital infrastructure and conducting a range of cyber intrusions and attacks against targets in the United States."[15] The federal government is issuing similar reports and warnings daily. At a hearing on this Motion, Plaintiffs will present expert testimony that makes plain to this Court what the U.S. government and private researchers already know — Georgia's voting system is a catastrophically open invitation to malicious actors intent on disrupting our democracy.

8. Conclusion – Plaintiffs are Likely to Succeed on the Merits

On the basis of the foregoing, as to Plaintiffs' fundamental right to vote claim (Count One), Plaintiffs are likely to succeed at trial on the merits by establishing with overwhelming evidence that Georgia's DRE voting system is extremely vulnerable to attack, by design is unverifiable, and has been further

[15] Remarks of D. Coats to Hudson Institute, July 17, 2018. Transcript available at https://www.npr.org/2018/07/18/630164914/transcript-dan-coats-warns-of-continuing-russian-cyberattacks. (Last viewed July 30, 2018).

compromised by the Defendants' neglect. Plaintiffs will further show that the risk that votes will be miscounted or diluted outweighs any interest of the State in insisting upon the continued use of these machines. *Crawford,* 553 U.S. at 190.

As to Plaintiffs' claim under the Equal Protection Clause (Count Two), Plaintiffs will likely succeed in establishing that users of DRE machines are "less likely to cast an effective vote" than users of paper ballots because of the foregoing vulnerability and flaws in the DRE voting system. *Wexler,* 452 F.3d at 1231.

B. Plaintiffs Are Likely to Suffer Irreparable Harm

The harm to Plaintiffs if the injunction is not granted is by its very nature irreparable. Voting is a "fundamental political right, because preservative of all rights." *Yick Wo v. Hopkins*, 118 U.S. 356, 370 (1886). There will be no remedy – through damages or otherwise – if the DRE system fails to issue correct ballots or count the votes in the November and December 2018 elections correctly.

Defendants may contend that Plaintiffs cannot prove to a metaphysical certitude that the DREs will miscount their votes. This argument misstates the legal test and miscomprehends the nature and extent of the threatened injuries. First, the test for granting equitable relief is not whether injury is certain to occur, but whether it is "likely" to occur. *Winter,* 555 U.S. at 20. Plaintiffs have shown that, unless this injunction is granted, the legitimacy of Georgia's election results will be cast into doubt and irreparable harm is likely to occur to the right of voters

to have their votes correctly counted. Second, the likely miscounting of *any* votes infringes upon Plaintiffs' constitutional rights. *Anderson v. United States*, 417 U.S. 211, 226 (1974) (Marshall, J.) ("The deposit of forged ballots in the ballot boxes, no matter how small or great their number, dilutes the influence of honest votes in an election, and whether in greater or less degree is immaterial.").

Third, Georgia's use of paperless electronic voting system undoubtedly increases the risk of irreparable harm, and the increased risk of harm constitutes actual injury. *See Monsanto Co. v. Geerston Seed Farms*, 561 U.S. 139, 153-154 (2010) ("A substantial risk of gene flow injures respondents in several ways"); *Massachusetts v. E.P.A.,* 549 U.S. 497, 526 (2007) ("The risk of catastrophic harm, though remote, is nevertheless real."); *Farmer v. Brennan*, 511 U.S. 825, 828 (1994) ("'A prison official's 'deliberate indifference' to a substantial risk of serious harm to an inmate violates the Eighth Amendment."). Indeed, the actual harm with respect to Plaintiffs' equal-protection claim is the increased risk that DRE votes will not be counted correctly or verified in post-election challenges relative to verifiable paper ballots. *Wexler,* 452 F.2d at 1231. That harm – the increase in the risk - is certain to occur.

Finally, the widespread acceptance of the legitimacy and accuracy of an election is itself a value that is certain to be irreparably harmed if the election goes forward using Georgia's profoundly vulnerable and concededly unverifiable

system. What Judge Biery said in *Casarez v. Valverde County* over twenty years ago unquestionably remains true today: "'Those who have studied history and have observed the fragility of democratic institutes in our own time realize that one of country's most precious possessions is . . . widespread acceptance of election results.'" 957 F. Supp. 847, 865 (W.D. Tex. 1997) (citation omitted).

C. Balance of Equities Favors Granting the Injunction

The balance of equities tips heavily in Plaintiffs favor. On the one hand, the weight of Plaintiffs' equities is substantial. "No right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined." *Wesberry,* 376 U.S. at 17.

On the other hand, the injunction will not cause Defendants substantial harm, but will merely require Defendants to do what every federal agency on record has urged the State to do: use paper ballots to record votes. An injunction also will not cause Defendants to do anything new. Defendants already record votes by paper ballot and count them by optical scanner or by hand; the injunction will of course cause a substantial increase in the number of votes cast by paper ballot, but the actual burden of this change on the Defendants will be slight.

Indeed, the cost of additional paper ballots and associated supplies (felt tip pens, cardboard privacy screens) is likely to be more than offset by the savings

associated with not having to deploy tens of thousands of labor-intensive DRE machines. The State of Maryland in 2016 switched from the type of DRE machines that Georgia uses to the paper ballot/optical scanner process that would be deployed if this preliminary injunction were granted. Rebecca Wilson, Chief Election Judge at Precinct 17-01 in Prince George's County, Maryland, states in her declaration that Maryland's paper ballot system "is far easier and faster to set up, manage and close down" than were the previous DRE machines. (Wilson Decl. ¶ 5). Ms. Wilson's highly detailed declaration shows how the number of steps necessary to set up and close down the paper ballot and optical scanning system is a small fraction of the effort to set up and close down the DRE machines in her precinct. (Wilson Decl. ¶¶ 6-12). Wilson further explains that it took little or no pollworker training to make the switch, and that "[v]oters have expressed to me that they were happy with the new paper balloting equipment." (Wilson Decl. ¶¶ 13-17, 26). Indeed, even this framing of the issue is overly generous to Defendants, for these cost estimates do not measure the astronomical cost to the State if the election is hacked.

Finally, District Courts have repeatedly found that fundamental voting rights outweigh the administrative cost associated with fixing election systems or procedures. An illustrative case is *NAACP v. Cortes,* 591 F. Supp. 2d 757 (E.D. Pa. 2008). In *Cortes,* the plaintiff sued seven days before the 2008 general

election, seeking an injunction addressing Pennsylvania's contingency plans in the event that the DREs in a polling place malfunctioned. The District Court granted the injunction and issued an order requiring the Secretary of the Commonwealth to direct County Boards to distribute paper ballots whenever 50% of the electronic voting machines in a precinct became inoperable. The District Court rejected as factually unfounded the defendants' arguments that changing the rule as to use of paper ballots would "cause chaos and confusion," and that poll workers had not been trained as to the simultaneous use of paper ballots and DRE machines. While the court agreed that the suit was filed "at the eleventh hour," the court found that "the granting of injunctive relief as requested will cause minimal harm to defendants." 591 F. Supp.2d at 763, 768.

Other district courts have reached the same conclusion in cases involving election systems and processes. "Although these reforms may result in some administrative expenses for Defendants, such expenses are likely to be minimal and are far outweighed by the fundamental right at issue." *United States v. Berks County*, 250 F. Supp. 2d 525, 541 (E.D. Pa. 2003) (granting preliminary injunction); *see also Johnson v. Halifax County,* 594 F. Supp. 161, 171 (E.D.N.C. 1984) (granting preliminary injunction, finding that administrative and financial burdens on defendant not undue in light of irreparable harm caused by unequal opportunity to participate in county election).

D. Injunction Is in the Public Interest

The requested relief is in the public interest because it is in accord with the unanimous, and urgent, recommendations from officials at the highest levels of the Federal Government. In addition, public confidence in Georgia's election systems will be greatly enhanced by the granting of the requested relief. "'The public must have confidence that the election process is fair.'" *Casarez,* 957 F. Supp. at 865 (granting preliminary injunction in election case) (citation omitted). The preliminary injunction requested by the Coalition Plaintiffs is manifestly in the public interest.

IV. CONCLUSION

For the foregoing reasons, the Motion should be granted.

This 3rd day of August, 2018.

/s/ Bruce P. Brown
Bruce P. Brown
Georgia Bar No. 064460
BRUCE P. BROWN LAW LLC
Attorney for Coalition for Good Governance
1123 Zonolite Rd. NE
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

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

/s/ William Brent Ney
William Brent Ney
Georgia Bar No. 542519
Attorney for Coalition
for Good Governance, William
Digges III, Laura Digges,
Ricardo Davis, and Megan
Missett
NEY HOFFECKER
PEACOCK & HAYLE, LLC
1360 Peachtree Street NE
Atlanta, Georgia 30309
(404) 842-7232

/s/ Cary Ichter
CARY ICHTER
Georgia Bar No. 382515
Attorney for Coalition
for Good Governance, William
Digges III, Laura Digges,
Ricardo Davis and Megan
Missett
ICHTER DAVIS LLC
3340 Peachtree Road NE
Suite 1530
Atlanta, Georgia 30326
(404) 869-7600

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

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF COMPLIANCE

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

/s/ Bruce P. Brown
Bruce P. Brown
Georgia Bar No. 064460
BRUCE P. BROWN LAW LLC
Attorney for Coalition for
Good Governance
1123 Zonolite Rd. NE
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

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

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF SERVICE

This is to certify that I have this day caused the foregoing COALITION PLAINTIFFS' BRIEF IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION to be served upon all other parties in this action by via electronic delivery using the PACER-ECF system.

This 3RD day of August, 2018.

/s/ Bruce P. Brown
Bruce P. Brown
Georgia Bar No. 064460
BRUCE P. BROWN LAW LLC
Attorney for Coalition for
Good Governance
1123 Zonolite Rd. NE
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

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

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATIONS IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

August 3, 2018

DECLARATION OF MATTHEW D. BERNHARD

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

DONNA CURLING, et al.	)	
	)	
Plaintiff,	)	
	)	**CIVIL ACTION FILE NO.:**
vs.	)	**1:17-cv-2989-AT**
	)	
BRIAN P. KEMP, et al.	)	
	)	
Defendant.	)	
	)	

DECLARATION OF MATTHEW D. BERNHARD

MATTHEW D. BERNHARD ("Declarant") hereby declares as follows:

1. I am Ph.D. candidate at the University of Michigan in Computer Science with a focus on computer security. I received my Bachelor's degree from Rice University, and my Master's in Computer Science from the University of Michigan.

2. I have focused my study in the field of computer science, including cyber-security in voting systems since 2012, including specific work on new, secure voting technology (the STAR-Vote system from Austin, Texas). I have worked with the Verified Voting Foundation on gathering data about currently deployed voting systems. I consulted with the Jill Stein recount campaign in 2016 to assess threat models and incident reports in Michigan, Wisconsin, and Pennsylvania. I have also worked with other experts in the field to provide a theoretical survey of properties of election security.

3. Following the 2016 recount, I, along with a colleague, performed a statistical analysis of the data generated in the 2016 recounts in Wisconsin and Michigan. Our findings highlighted a lack of strong evidence towards concluding that the 2016 election was sufficiently secured in those states, as well as highlighting some anomalous data. For example, our findings indicated that the Optech IIIP-Eagle machines in use in some Wisconsin counties had a significantly high error rate. These machines were subsequently decertified and taken out of use in Wisconsin. We also found significant anomalies in Michigan's Wayne County, owing to the fact that the chain of custody had been compromised in almost half of precincts. In response to

these anomalies, the state launched an investigation into Wayne county and subsequently purchased new voting equipment for the whole of the state.

4. During the last 8 months I have conducted focused research on Diebold AccuVote voting system, of the type used by Georgia, with a specific emphasis on TS and TSX machines. That research has included in-lab testing at the University of Michigan on machines acquired through eBay, during which we performed an in-depth technical analysis of the systems and found significant vulnerabilities. I have also on several occasions observed AccuVote units in the field in Georgia, both at the Fulton County Election Preparation Center on multiple occasions and at the Grady High School precinct during an election. As with lab testing, I observed a significant number of operational vulnerabilities that make Georgia's election infrastructure fundamentally unsafe and untrustworthy.

5. I have published and spoken extensively about the cybersecurity and other risks of electronic voting systems and have assisted in preparation of other experts for Congressional testimony concerning these topics.

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

The Inherent risks of paperless electronic voting machines

7. Paperless voting machines, of the type used in Georgia, directly record votes to an electronic storage medium. Such machines are called Direct Recording Electronic voting machines, or DREs for short.

8. As DREs only record votes to an electronic medium, e.g. a USB stick, a voter has no way of independently verifying that the button they touched on the screen is what the machine recorded in memory. Other voting mechanisms, like paper ballots, provide this feature, which is called a voter-verifiable paper audit trail (VVPAT). VVPATs allow voters to check that the vote cast is the vote they intended, independent of the system itself.

9. As DREs do not have this feature, it is impossible for a voter to check that their vote was recorded as they intended. Since voters are stored solely in memory, if something in the software were causing votes to be misrecorded, such an error could similarly cause the system to misreport that it was correctly recording votes. If the system is not correctly recording votes, either in error or out of malice, there is no way to tell. Any assurance provided by the machine would be akin to a criminal insisting that he did not commit the crime---other evidence is needed to corroborate the claim.

10. Because DREs provide no way to independently verify that votes are correctly recorded, security experts strongly recommend against their use with near unanimity, a recommendation with which I concur.

11. DREs are essentially just regular computers, often running the same software as a commodity laptop. Like any regular computer, DREs are vulnerable to any kind of malicious

exploitation, and in fact often moreseo as they typically run out-of-date software that lacks critical security patches. Exploitable vulnerabilities in DREs run the full gamut: buffer overflows in the vote recording software, privilege escalation bugs in the operating system, improper checksum verification by the bootloader, and architectural flaws such as improper use of voter authentication technologies are just a few examples at various levels of the DRE system. Using one of these exploitations, an attacker can make the DRE do just about anything. For example, my academic advisor made one such DRE, the Sequoia AVC Edge, run Pac-Man. There is nothing different about Georgia's voting system that would prevent a similar exploitation. This level of vulnerability makes it exceedingly possible for DREs to be infected with software that does not accurately record votes.

12. Since DREs have no way to independently verify votes as recorded, any software that could change votes could do so undetected. Since DREs are not made available for public auditing, there is no way to determine if their software has been modified in anyway. Even if such an audit were to be performed, it is still not certain that it would definitively prove the machines are free from infection. As such, for the individual voter and election official, there is no way to know that a DRE machine has accurately recorded votes. These machines could essentially output random results and, barring results that prove surprising in light of other evidence, no one would know. Worse, even if suspicions about incorrect election results were raised, DREs provide no recourse to explore, detect, or correct for these mistakes. In short, DREs are in no way fit to be trusted with any election process.

ACADEMIC RESEARCH ON DIEBOLD VOTING SYSTEMS

13. Other experts in the field of voting system security and computer science and I rely on a body of academic research conducted over the years that includes the following key reports as summarized in paragraphs 14 through 25.

14. Kohno et al.'s 2004 "Analysis of an Electronic Voting System"[1] report is the first independent security analysis of a Diebold voting system that I am aware of. The report focuses on the election management system (EMS) and AccuVote TS machine, the same that is used in Georgia. The report's authors found that it is possible to create voter access cards which enable the voter to vote an unlimited number of times. The report also highlighted numerous vulnerabilities in the source code that can be exploited to gain complete control over the voting system as well as show how each voter voted. This report spurred the commissioning of additional analyses of the AccuVote TS by the states of Ohio (Compuware[2]) and Maryland (SAIC[3], RABA[4]). All of these reports corroborated the findings of Kohno et al., even implementing voter access cards granting unlimited votes.

[1] http://avirubin.com/vote.pdf
[2] https://www.verifiedvoting.org/wp-content/uploads/2016/11/01-compuware112103.pdf
[3] https://elections.maryland.gov/pdf/risk_assessment_report.pdf
[4] http://euro.ecom.cmu.edu/program/courses/tcr17-803/TA_Report_AccuVote.pdf

15. An independent study on behalf of Blackbox Voting was conducted by Harri Hursti in 2006,[5] following the work of Kohno et al. This study looked exclusively at the AccuVote TS and TSX machines. This report explains the vulnerabilities present in Windows CE, the operating system of the machines, which provides almost no security beyond what an application itself can provide. Essentially, rather than attacking the voting software itself, an attacker can attack the operating system to completely control the system, or, at a lower level, the bootloader. The report also notes that the machine lacks physical security: with just a Philips head screwdriver an attacker can completely circumvent the locks and seals meant to protect the internals of the machine. With this level of vulnerability, an attacker can coerce the voting machine into doing anything.

16. A contemporaneous 2006 study done at Princeton by Feldman et al.[6] examined just the AccuVote TS. This study confirmed findings of prior work. Additionally, this study implemented a new attack, whereby software designed to steal votes (a virus) is installed on the machine by exploiting the vulnerabilities highlighted in previous work. Once on the machine, the virus can completely change votes, and additionally make copies of itself onto any removable media that is plugged into the machine. In this way, an attacker with access to only one voting machine can potentially infect an entire precinct, county, or in Georgia's case, state, as the software reproduces in an exponential fashion with each new infection. Some of the vulnerabilities highlighted in the study are hardware-based, and thus not patchable. These vulnerabilities exist in the machines to this day. The study also found that logic and accuracy testing and parallel testing, methods to detect and reduce machine errors, do not detect any malicious behavior by the machine.

17. Kiayias et al., researchers from the University of Connecticut,[7] built on Hursti and Feldman et al., designing an attack against the AccuVote TSX machine that could swap candidate order or remove a candidate from the ballot by exploiting many of the vulnerabilities pointed out in the earlier studies.

18. The Top-to-Bottom Review (TTBR),[8] commissioned by the State of California in 2007, found that every component of Diebold voting systems, of the type used in Georgia, were riddled with vulnerabilities. With access only to the election management system (EMS, called GEMS by Diebold) and a few of the machines, researchers found vulnerabilities which, if exploited, permit attackers to gain full access to the election management system and complete control of individual voting machines, including the ability to surreptitiously add, delete, or change votes. The EMS was found to have insufficient passwords, integer overflow bugs, no security enforcement outside the graphical user interface, and lack of critical security patches to the Windows operating system it runs on. Essentially, an attacker could modify any data in the EMS (ballot styles, vote databases, etc.) as well as gain control of the operating system. The TTBR corroborated prior work about significant, numerous vulnerabilities in the voting machines and expanded it, finding a lack of input validation in voter-accessible fields that lead to

[5] https://www.blackboxvoting.org/BBVtsxstudy.pdf
[6] https://jhalderm.com/pub/papers/ts-evt07.pdf
[7] http://www.votetrustusa.org/pdfs/Diebold%20Folder/TSX_Voting_Terminal_Report-UConn.pdf
[8] http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/

erratic behavior, privilege escalation that would enable a voter to gain full administrative control over the voting machine with little to no effort, and that election administrator credentials can be extracted from the memory cards used to store votes during the close of election process. The TTBR also found that the machines expose how voters vote.

19. The EVEREST report[9] commissioned by the State of Ohio in 2007 corroborated the TTBR and found similar issues in Premier (Diebold) systems. In addition to further confirming prior work, EVEREST also examined ExpressPoll books, computers used to verify voter registration data and authorized voters to vote on election day. The ExpressPoll, considered to be a critical component of Georgia's DRE election system, was found to have similar vulnerabilities to the other systems already studied: lack of security patches, unencrypted voter records, and insecure booting procedures that allow an attacker to run any software, including malware, on the unit. EVEREST also found new vulnerabilities in GEMS and the AccuVote TSX, including key reuse, unauthenticated log access (anyone can forge an audit log), a shared SSL certificate between the EMS and TSX, allowing an attacker to impersonate the EMS and upload fake election results, lack of accurate security protections on data keys, BIOS password reuse that would allow an attacker to run arbitrary software, and unpatched operating system vulnerabilities that allow an attacker to gain full access to the EMS or voting machine.

20. The Florida Department of State commissioned a study of Diebold voting software in 2007[10] to examine Diebold election management software, touch-screen voting machines, and optical scan voting machines. This report was independent and contemporaneous with the EVEREST and TTBR reports. The study focused only on corroborating prior vulnerability findings from Hursti, Feldman et al., Kohno et al., Ohio's Compuware assessment, and Maryland's RABA and SAIC reports. The study found that some issues from prior source code reviews had been fixed in in-the-field machines, but many other attack vectors, like unlimited votes with smart cards or operating system vulnerabilities had not been fixed and still presented an avenue for attack.

21. All of these studies explore electronic voting systems used in Georgia. Much of the research was conducted on BallotStation versions 4.3, 4.4.1, and 4.6.4. While the version used in Georgia, 4.5.2! has a high overlap in functionality and form to these previously studied systems, it is not known how much functionality, and by extension vulnerability, overlap. However, given that many of the vulnerabilities above rely on the architecture of the voting system, not particular features of the software, it is almost certain that they apply to Georgia's system.

22. A few cursory examples of vulnerabilities that apply to Diebold software, regardless of version, include the smartcard vulnerabilities, wherein any malicious party can craft a smartcard that impersonates a voter access card but which ignores the machine's command to deactivate itself. In effect, voter cards which allow an unlimited number of votes are still possible in the Georgia system.

[9] http://www.patrickmcdaniel.org/pubs/everest.pdf
[10] http://nob.cs.ucdavis.edu/bishop/notes/2007-fsusait-2/2007-fldiebold.pdf

23. Georgia's system still runs on Windows CE, an operating system which has not been supported in 5 years. This means that critical security patches that would mitigate some of the lower-level attacks proposed and implemented above simply do not exist. As the operating system is over twenty years old, it lags behind the two decades of computer security research and is extremely vulnerable to a wide variety of attacks that Diebold's software, regardless of version, cannot defend against. If Diebold's software is a house, the operating system is the foundation upon which the house is built. No amount of drywall repair can fix a cracked foundation.

24. Georgia's voting machine are still programmed using PCMCIA memory cards, and any piece of software hosted on such a memory card can infect the voting machine, as the Princeton study demonstrated. Officials are quick to claim that the machines are not connected to the Internet, and therefore secure, but as we have witnessed in the Stuxnet episode[11] as well as recent Russian attempts to infiltrate other critical infrastructure,[12] this does not prevent malware from coming in contact with the voting machines.

25. Finally, the fundamental architecture of Georgia's voting machines, specifically the AccuVote TS and AccuVote TSX, prevent them from providing reliable evidence that the election results they produce are correct. Votes merely exist on memory cards, and any source of error, malice, or act of god can change the votes and leave absolutely no indication that such a change has occurred. Even if such a change were detected, all original evidence of voter intent no longer exists, so it is not possible to reconstruct a correct election result. In short, Georgia's voting machines fail to meet the burden of proof for accurate, verifiable election outcomes: a durable record of voter intent. For this reason, these machines are unfit for use in any electoral context.

MY STUDY OF DIEBOLD VOTING MACHINES

26. In recent months my academic advisor and I have begun replicating past research into AccuVote TS and TSX machines, as well as attempting to find new vulnerabilities in more recent versions of the software. As Georgia's software is totally unavailable, my efforts have primarily focused on BallotStation 4.7.

27. We have successfully recreated the unlimited voter access card attack, and I am confident that, given just a few seconds with access to one of Georgia's voting machines, I could very easily produce a card that would let any Georgia voter vote as many times as they would like.

28. We have observed that more recent versions of the voting software application, BallotStation, does include fixes for some of the more egregious vulnerabilities found in prior

[11] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[12] https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110

work. For instance, votes are no longer stored completely in plaintext, and the cryptographic key used on each machine is now no longer the same. However, the fixes put in place are fairly easily defeated: malware can read the keys out of memory and decrypt votes.

29. The physical security of the machines is easily defeated. The AccuVote TS machines have their memory cards and power buttons protected by a lock that is keyed by the same key used in minibars and jukeboxes, which is readily available for purchase online. Failing this, the locks can be picked in under 10 seconds. The power button and memory card are protected in a similar fashion on the TSX, however the lock used on that machine is a cylindrical lock. I can pick this lock in less than ten seconds with nothing but a BIC pen. Video of my first attempt at this can be found here: https://www.youtube.com/watch?v=vqNJL0fYwSk.

30. Vote-stealing software that changes votes in an undetectable way has been put on TSX machines by my advisor and I, targeting the 4.6.4 version of BallotStation. We demonstrated this for the New York Times here: https://www.nytimes.com/video/opinion/100000005790489/i-hacked-an-election-so-can-the-russians.html

31. We have observed that the seals used to secure individual voting machines after the close of polls may be purchased on Amazon[13]. If an attacker were to break off a seal, it would be easy to simply replace it, and etch the serial number of the broken seal on the replacement seal. The same can be said for the cable ties used to secure the voting machines in a precinct to each other.

32. In short, with even a short window of access to one of Georgia's voting machines, it would be easy for an attacker to install undetectable vote-stealing software. I have personally observed Georgia election workers leave voting equipment unattended and insufficiently sealed to prevent tampering within the last 30 days.

33. Due to the architectural flaws of the system, and failures in operational security at many levels, it is not possible for any person to faithfully attest that each voting machine in the state of Georgia is free from malware that could affect election results.

NEED FOR SECURE FACILITIES

34. After the primary on Tuesday, July 24th, 2018, I and my colleagues observed the close of polls at Grady High School in Atlanta, Georgia. After the poll workers had closed down the polling place, they stacked the voting machines and sealed them. At this point, they all left the gym, leaving myself and my colleagues alone with the voting machines, with only one security camera watching over us. It would have been very easy for an attacker to disable the camera and modify the voting machines without detection. As the results of the Princeton study demonstrate, it only takes one lapse for a virus to propagate from machine to machine, silently changing votes all over the state of Georgia. As mentioned above, the seals and cable locks on

[13] https://www.amazon.com/Blue-Pull-Tite-Security-Seal-Package/dp/B008CFSHJG

the machines are available for purchase, so they provide no security against this kind of attack.

35. I have also on several occasions visited the Fulton County Election Preparation Center in 2017 and 2018. On several occasions, I was allowed to roam the warehouse where all of Fulton County's voting machines are programmed, serviced, and stored, as well as where election night results are tabulated and published. The facility was wholesale lacking in operational security necessary to protect Georgia's machines from tampering or misuse.

36. In the Fulton County Election Preparation Center warehouse, I witnessed

a. stacks of voter access and supervisor cards that could easily be stolen, with no chain of custody to ensure none have left the facility,

b. printouts of password sheets are pasted all over the facility, divulging passwords that would allow anyone to render voting machines unusable,

c. stacks of memory cards were strewn about during the election programming process, as many cards are programmed at once using card replicators. If a virus were present on even one of these memory cards, the card replicators would ensure that the virus could spread even more quickly than first imagined in the Princeton study,

d. I was able to learn the three-digit password for the code-protected door into the facility while being invited in by a poll worker, and

e. the election prep center has no surveillance on its exterior, save for a motion detector, and the security cameras inside the facility are often obstructed by the high warehouse shelves.

37. In Fulton County, votes are transmitted on election night from annexes via modem, meaning that all ballots from the annexes are sent unencrypted to the tabulation server. An employee reported that occasionally the phone lines leading into the tabulation server receive telemarketing calls.

38. Votes transmitted via modem are routed using AccuVote TSX machines into the tabulation server. Given the vulnerabilities present in the machine, any malware resident on these machines could very efficiently change election results.

39. In June of 2018 at the Fulton County Election Preparation Center, I observed the logic and accuracy testing performed on the voting machines before they are sent to their precincts. These tests are fully automated, and could be easily defeated by malware that simply kept track of the date. In 2015, it came to light that Volkswagen had written software in their cars

to fool emissions tests in just this way, and a voting machine logic and accuracy test is far more simple than an automobile emissions test.[14]

40. I understand that four poll books in Georgia were stolen in April 2017[15]. This raises additional security concerns. The poll books contain an encryption key to generate voter access cards (VACs). Someone in possession of the poll books could, thus, extract these keys and use them later to generate VACs that could be used to cast illegal votes, as discussed above. To address the threat posed by this breach of security, it would be necessary to generate new encryption keys and install them in all poll books and voting machines.

ADVANCED PERSISTENT THREAT

41. Advanced Persistent Threats (APTs) are cyber attackers that specialize in gaining unauthorized access to system and maintain that access over a long period of time, undetected. In order to defend against these kinds of attackers, an incredibly high level of security discipline is required. After a period of vulnerability, it is a significant effort to identify the presence of APTs and successfully eliminate their access.

42. Advanced Persistent Threat actors often try to penetrate critical infrastructure systems in order to gain access, gather intelligence, and gain the ability to create damage at a time of their choosing. As one example, Exhibit B is an FBI bulletin from 2013 on Advanced Persistent Threat actors' attacks against the aviation sector. Exhibit C is a more recent alert from the Department of Homeland Security, revised on August 23, 2017, detailing activities by "actors of the North Korean government to target the media, aerospace, financial, and critical infrastructure sectors in the United States and globally."

43. Given my knowledge and study of cybersecurity as it pertains to voting systems, it is extremely likely that APTs are trying to access and manipulate election systems. Given the level of vulnerability present in Georgia's voting system, it is a near certainty that if an APT has tried to get in, it has succeeded. As I myself have gained access to Georgia's election system, it is certainly true that a well resourced and motivated attacker could do so as well.

44. A massive, time-consuming effort would be required to address the security breaches that occurred in Georgia, requiring experienced technicians to give hands-on attention to individual machines (tens of thousands of pieces of equipment), one at a time. The memory cards also would need to be disinfected or replaced. Such an effort could mitigate the potential effects of past breaches but future breaches would still be possible.

---

[14] https://arstechnica.com/cars/2015/12/vw-says-rulebreaking-culture-at-root-of-emissions-scandal/

[15] https://www.ajc.com/news/state--regional-govt--politics/voters-personal-data-risk-cobb-theft/FYDyqME5bqLG4ip4snYLwO/

45. Due to the apparent lack of chain of custody of election equipment in Georgia, specifically voter cards and memory cards, Georgia would have to first provide a way to exhaustively inventory every piece of election equipment in its possession, and then meticulously scrub each component to ensure no malware persists. Such an effort would be enormously costly, and potentially not possible.

46. Even if such a task could be completed, if at any time in the future another exposure or breach occurs, the entire process would have to be repeated, again at enormous cost.

47. Because of the vulnerability of Georgia's voting system to software manipulation, and because of intelligence reports about APTs having attempted to affect elections in the United States, such precautions appear to be necessary in Georgia. Without significant effort to detect and revoke access to attackers, the ability for Georgia's voting systems to correctly carry out elections should be viewed with even greater skepticism.

48. DREs are fundamentally unable to provide sufficient evidence that the election results they produce are correct. Given Georgia's reliance on these machines, and known security breaches in 2016 and 2017, and the significant challenges to mitigate current vulnerabilities in the system, it is my opinion that Georgia, in order to effectively run its elections, must abandon its DREs prior to the upcoming November election.

49. I have reviewed the affidavits and exhibits listed in paragraph _____ of the Motion for Preliminary Injunction, as well as additional documentation of numerous similar irregularities from recent elections. The errors reported are consistent with the kinds of errors I would expect to see generated by malware, programming errors, or other sources of computer system malfunction. The Diebold DRE system, including the ExpressPollbook, is known to be vulnerable to malicious manipulation that would produce such errors. Without a forensic examination of the machines involved in the reports, the reported errors cannot be explained to any degree of certainty. In some cases, the lack of a reliable audit trail and the ability for malicious users to install undetectable malware could result in the original source of the irregularities and malfunctions being indeterminable even in spite of a forensic examination.

50. I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, August 3, 2018.

Matthew D. Bernhard

EXHIBIT A

Exhibit A

Matthew D. Bernhard
matber@umich.edu

2260 Hayward Street
Ann Arbor, MI 48109
Main/Cell: 281-725-8544

EDUCATION

University of Michigan, Ann Arbor, MI (2015 – present)
PhD Candidate Student, Computer Science and Engineering
Advisor: J. Alex Halderman
University of Michigan, Ann Arbor, MI (2015 – 2018)
Master of Science, Computer Science and Engineering
Rice University, Houston, TX (2012 – 2015)
Bachelor of the Arts, Computer Science
Advisor: Dan Wallach

EXPERIENCE

Verified Voting – 2018 - present
Data Science Consultant, Ann Arbor, MI
- Collected, organized, and wrote up technical information about new voting machines being acquired by localities

Cloudflare – San Francisco, CA
Cryptography Intern, *Summer 2017*
- Developed Certificate Transparency monitoring features. Also built an SSL detector to determine what SSL settings customer sites can support.

Computer Security Lab – Rice University, Houston TX
Lead Software Developer**,** Fall 2012 - Spring 2015
- Lead a team in upgrading and maintaining STAR-Vote, a pedagogical voting system
- Performed usability study on ballot preparation tool
- Explored leveraging utilities provided by the Chromium project to process sandbox and enforce tighter systems controls
- Examined secure data structures such as authenticated dictionaries for implementing a secure web bulletin board

Microsoft Research – Microsoft, Redmond WA
Research Intern, *Summer 2015,* Advised by Josh Benaloh
- Investigated trusted computing features in the Windows operating system
- Designed ASKVote, the Auditably Secure Voting scheme to provide software assurance and election evidence
- Designed voting client for conference demonstration hall survey

TEACHING

Introduction to Computer Security – University of Michigan
Graduate Student Instructor**,** Winter, 2018
- Lectured, led discussion section, graded, and provided course support.

Securing Digital Democracy – University of Michigan, Coursera
Course Operations Liaison**,** 2014 – 2018

- Compiled and maintained course resources and facilitated student discussion in message boards for course introducing the field of voting technology in the context of computer security

Fundamentals of Parallel Programming – COMP 322, Rice University
Teaching Assistant, Spring 2015

- Shaped curriculum and led lab discussions for an introductory course on parallel programming featuring Java parallelism and Apache Spark

Introduction to Program Design – COMP 215, Rice University
Teaching Assistant, Fall 2014

- Led lab discussions and wrote and reviewed assignments and exams for an introductory course on Java and Object Oriented Programming

PEER-REVIEWED PUBLICATIONS

403 Forbidden: A Global View of Geoblocking
Allison McDonald, Matthew Bernhard, Benjamin VanderSloot, Will Scott, J. Alex Halderman, Roya Ensafi
To appear at the ACM Internet Measurement Conference 2018 (IMC '18), Boston, Massachussetts. November 2018.

Voting Technologies, Recount Methods and Votes in Wisconsin and Michigan in 2016
Walter R. Mebane, Jr. and Matthew Bernhard
Proc. of the 3rd Workshop on Advances in Secure Electronic Voting (Voting '18). Nieuwpoort, Curaçao. March 2, 2018.

Public Evidence from Secret Ballots
Matthew Bernhard, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, Dan S. Wallach
Proc. of the Second Annual Joint Conference on Electronic Voting (E-Vote-ID '17). Bregenz, Austria. October 24 - 27, 2017.

Understanding the Mirai Botnet
Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever,Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, Yi Zhou
Proc. of the 26th USENIX Security Symposium (USENIX Security '17). Vancouver, BC, Canada. August 16 - 18, 2017.

Towards a Complete View of the Certificate Ecosystem
Benjamin VanderSloot, Johanna Amann, Matthew Bernhard, Zakir Durumeric, Michael Bailey, and J. Alex Halderman
Proc. 16th ACM Internet Measurement Conference (IMC '16), Santa Monica, California. November 2016

Implementing Attestable Kiosks
Matthew Bernhard, Gabe Stocco, and J. Alex Halderman
Proc. 14th Annual Conference on Privacy, Security, and Trust (PST '16), Auckland, New Zealand. December 2016

SELECTED OTHER PUBLICATIONS

What Might Go Wrong in the 2016 Election
Matthew Bernhard and J. Alex Halderman
Security at Michigan (a Medium publication), November 7th, 2016
The Security Challenges of Online Voting Have Not Gone Away
Robert Cunningham, Matthew Bernhard, and J. Alex Halderman
IEEE Spectrum, November 3rd, 2016

TALKS

Do We Want to Recount or Not? Presidential Election 2016
Matthew Bernhard and Kimball Brace
Election Verification Network (EVN) Symposium 2017, March 15, 2017

Recount 2016: An Uninvited Audit of the U.S. Presidential Election
Matthew Bernhard and J. Alex Halderman
Roadsec 2017, São Paulo, Brazil, November 11th, 2017
Roadsec Pro 2017, São Paulo, Brazil, November 10th, 2017
Electoral Technology Workshop, SBSeg 2017, Brasília, Brazil, November 6th, 2017
33rd Chaos Communication Congress (33c3), December 28th, 2016

MEDIA APPEARANCES

NPR, Reuters, BBC News, The Guardian, Le Monde, Motherboard, Forbes, The New Republic, Gothamist, The New Political, The Outline, and Voice of America News and others

EXHIBIT B

FBI Cyber Division

Private Sector Advisory

July 10, 2013

(U//FOUO) APT Actors Increased Interest in the Aviation Industry

(U) General Observations

(U//FOUO) Since June 2013, the FBI has observed advanced persistent threat (APT) actors' increased interest in the aviation industry. APT actors have sent spear-phishing e-mails targeting individuals associated with the air travel industry. Some of the spear-phishing e-mails originated from a spoofed sender in an attempt to make the e-mail appear more legitimate. E-mail recipients should be aware of suspicious and potentially malicious e-mail attachments or links.

(U) Impact of APT Activity

(U//FOUO) Every organization is at risk of being the target of an APT attack. APT actors, who are semi-sophisticated and difficult to detect while on network systems, have already cost US entities hundreds of millions of dollars over the past decade as a result of harvesting enormous amounts of critical information including proprietary data, source code, negotiation tactics, and strategic operational plans. These actors have also breached networks containing sensitive national security information. Going forward, this activity can best be mitigated with paradigmatic shifts in cyber security.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) APTs versus Hackers/Cyber Criminals

(U//FOUO) Advanced persistent threat actors differ from common hackers or cyber criminals by conducting targeted, rather than opportunistic, attacks that seek precise information rather than monetary gain, more closely resembling espionage. While the activity cannot often be definitively linked to any particular nation state, the sophistication, resources, and types of information sought suggests governmental support.

(U//FOUO) A general overview of the process by which APT actors compromise networks and systems is detailed in the table below, the vector of infection being most crucial:

1 - Infiltration	Reconnaissance	Actors search open sources to identify and assess targets for collection and entities/relationships to exploit in the attack.
	Infection	Typically, well-crafted spear phishing e-mails with linked or embedded files containing malicious code serve as the intrusion vector.
2 - Persistence	Establish Backdoors	Attackers maintain network footholds by obtaining domain administrative credentials and moving laterally through a network, establishing multiple backdoors.
	Enumerate the Network	Persistent threat intruders laterally enumerate a network gathering valid credentials (user accounts and passwords) for multiple systems.
	Install Utilities	Attackers install any number of several malicious utilities necessary to maintain persistence and ultimately steal information.
	Escalate Privileges	With access and persistence established, intruders escalate their privileges and prepare for exfiltration.
3 - Exfiltration	Harvest Data	Specific documents and e-mails containing targeted data are collected and packaged into a single, encrypted, and password-protected compressed file.
	Exfiltration	The intruders exfiltrate the compressed file to another compromised system in their command and control infrastructure.
	Conceal Activity	Finally, intruders either attempt to clean up their tools, maintaining persistence, or set the attack in a dormant state to evade detection while maintaining access.

(U) Defending Against APT Activity

(U) When weighing available options pertaining to the implementation of appropriate mitigation strategies, organizations must begin by asking themselves the following:

- (U) If proprietary data, personally identifiable information (PII), research and development-related data, e-mail, or other critical information were stolen, what would the current and future consequences be?

- (U) Has my organization evaluated data criticality based on risk? What must be protected in the organization?

(U) To mitigate the threat of APT activity, DHS's United States Computer Emergency Readiness Team (US-CERT) recommends the following actions:

- (U) Audit what needs to be networked and remove ("air gap") vital information from networked devices to ensure data protection.

- (U) Monitor for and report on suspicious activity, such as spear phishing e-mails, leading up to significant events and meetings.

- (U) Educate users about social engineering and e-mail phishing related to high-level events and meetings.

- (U) Measure expected network activity levels so that changes in patterns can be more easily identified.

- (U) Always treat unsolicited or unexpected e-mail containing attachments or links with caution, even (and perhaps especially) when the e-mail appears related to known events or projects.

(U) Reporting Notice

(U) The FBI and US-CERT encourage recipients of this document to report information concerning suspicious or criminal activity to the local FBI field office. The FBI's 24/7 Strategic Information and Operations Center can be reached by telephone at 202-323-3300 or by e-mail at SIOC@ic.fbi.gov. FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm. US-CERT can be reached by telephone at 888-282-0870 or by e-mail at SOC@us-cert.gov. The US-CERT homepage can be found online at www.us-cert.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) Administrative Note: Law Enforcement Response

(U) Information contained in this product is for official use only. No portion of it should be released to the media, the general public, or over non-secure Internet servers. Release of this material could adversely affect or jeopardize investigative activities.

EXHIBIT C

NCCIC

Alert (TA17-164A)

HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure

Original release date: June 13, 2017 | Last revised: August 23, 2017

Systems Affected

Networked Systems

Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides technical details on the tools and infrastructure used by cyber actors of the North Korean government to target the media, aerospace, financial, and critical infrastructure sectors in the United States and globally. Working with U.S. Government partners, DHS and FBI identified Internet Protocol (IP) addresses associated with a malware variant, known as DeltaCharlie, used to manage North Korea's distributed denial-of-service (DDoS) botnet infrastructure. This alert contains indicators of compromise (IOCs), malware descriptions, network signatures, and host-based rules to help network defenders detect activity conducted by the North Korean government. The U.S. Government refers to the malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information related to HIDDEN COBRA activity, go to https://www.us-cert.gov/hiddencobra.

If users or administrators detect the custom tools indicative of HIDDEN COBRA, these tools should be immediately flagged, reported to the DHS National Cybersecurity Communications and Integration Center (NCCIC) or the FBI Cyber Watch (CyWatch), and given highest priority for enhanced mitigation. This alert identifies IP addresses linked to systems infected with DeltaCharlie malware and provides descriptions of the malware and associated malware signatures. DHS and FBI are distributing these IP addresses to enable network defense activities and reduce exposure to the DDoS command-and-control network. FBI has high confidence that HIDDEN COBRA actors are using the IP addresses for further network exploitation.

This alert includes technical indicators related to specific North Korean government cyber operations and provides suggested response actions to those indicators, recommended mitigation techniques, and information on reporting incidents to the U.S. Government.

For a downloadable copy of IOCs, see:

- IOCs (.csv)
- IOCs (.stix)

On August 23, 2017, DHS published a Malware Analysis Report (MAR-10132963) that examines malware functionality to provide detailed code analysis and insight into specific tactics, techniques, and procedures (TTPs) observed in the malware.

For a downloadable copy of the MAR, see:

- MAR (.pdf)
- MAR IOCs (.stix)

Description

Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of data while others have been disruptive in nature. Commercial reporting has referred to this activity as Lazarus Group[1] and Guardians of Peace.[2] DHS and FBI assess that HIDDEN COBRA actors will continue to use cyber operations to advance their government's military and strategic objectives. Cyber analysts are encouraged to review the information provided in this alert to detect signs of malicious network activity.

Tools and capabilities used by HIDDEN COBRA actors include DDoS botnets, keyloggers, remote access tools (RATs), and wiper malware. Variants of malware and tools used by HIDDEN COBRA actors include Destover,[3] Wild Positron/Duuzer,[4] and Hangman.[5] DHS has previously released Alert TA14-353A,[6] which contains additional details on the use of a server message block (SMB) worm tool employed by these actors. Further research is needed to understand the full breadth of this group's cyber capabilities. In particular, DHS recommends that more research should be conducted on the North Korean cyber activity that has been reported by cybersecurity and threat research firms.

HIDDEN COBRA actors commonly target systems running older, unsupported versions of Microsoft operating systems. The multiple vulnerabilities in these older systems provide cyber actors many targets for exploitation. These actors have also used Adobe Flash player vulnerabilities to gain initial entry into users' environments.

HIDDEN COBRA is known to use vulnerabilities affecting various applications. These vulnerabilities include:

- CVE-2015-6585: Hangul Word Processor Vulnerability
- CVE-2015-8651: Adobe Flash Player 18.0.0.324 and 19.x Vulnerability
- CVE-2016-0034: Microsoft Silverlight 5.1.41212.0 Vulnerability
- CVE-2016-1019: Adobe Flash Player 21.0.0.197 Vulnerability
- CVE-2016-4117: Adobe Flash Player 21.0.0.226 Vulnerability

DHS recommends that organizations upgrade these applications to the latest version and patch level. If Adobe Flash or Microsoft Silverlight is no longer required, DHS recommends that those applications be removed from systems.

The IOCs provided with this alert include IP addresses determined to be part of the HIDDEN COBRA botnet infrastructure, identified as DeltaCharlie. The DeltaCharlie DDoS bot was originally reported by Novetta in their 2016 Operation Blockbuster Malware Report.[7] This malware has used the IP addresses identified in the accompanying .csv and .stix files as both source and destination IPs. In some instances, the malware may have been present on victims' networks for a significant period.

Technical Details

DeltaCharlie is a DDoS tool used by HIDDEN COBRA actors, and is referenced and detailed in Novetta's Operation Blockbuster Destructive Malware report. The information related to DeltaCharlie from the Operation Blockbuster Destructive Malware report should be viewed in conjunction with the IP addresses listed in the .csv and .stix files provided within this alert. DeltaCharlie is a DDoS tool capable of launching Domain Name System (DNS) attacks.

Network Time Protocol (NTP) attacks, and Carrier Grade NAT (CGN) attacks. The malware operates on victims' systems as a svchost-based service and is capable of downloading executables, changing its own configuration, updating its own binaries, terminating its own processes, and activating and terminating denial-of-service attacks. Further details on the malware can be found in Novetta's report available at the following URL:

https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf

Detection and Response

HIDDEN COBRA IOCs related to DeltaCharlie are provided within the accompanying .csv and .stix files of this alert. DHS and FBI recommend that network administrators review the IP addresses, file hashes, network signatures, and YARA rules provided, and add the IPs to their watchlist to determine whether malicious activity has been observed within their organization.

When reviewing network perimeter logs for the IP addresses, organizations may find numerous instances of these IP addresses attempting to connect to their systems. Upon reviewing the traffic from these IP addresses, system owners may find that some traffic corresponds to malicious activity and some to legitimate activity. System owners are also advised to run the YARA tool on any system they suspect to have been targeted by HIDDEN COBRA actors. Additionally, the appendices of this report provide network signatures to aid in the detection and mitigation of HIDDEN COBRA activity.

Network Signatures and Host-Based Rules

This section contains network signatures and host-based rules that can be used to detect malicious activity associated with HIDDEN COBRA actors. Although created using a comprehensive vetting process, the possibility of false positives always remains. These signatures and rules should be used to supplement analysis and should not be used as a sole source of attributing this activity to HIDDEN COBRA actors.

Network Signatures

alert tcp any any -> any any (msg:"DPRK_HIDDEN_COBRA_DDoS_HANDSHAKE_SUCCESS"; dsize:6; flow:established,to_server; content:"|18 17 e9 e9 e9 e9|"; fast_pattern:only; sid:1; rev:1;)

---

alert tcp any any -> any any (msg:"DPRK_HIDDEN_COBRA_Botnet_C2_Host_Beacon"; flow:established,to_server; content:"|1b 17 e9 e9 e9 e9|"; depth:6; fast_pattern; sid:1; rev:1;)

YARA Rules

{

meta:

description = "RSA Key"

strings:

$rsaKey = {7B 4E 1E A7 E9 3F 36 4C DE F4 F0 99 C4 D9 B7 94

A1 FF F2 97 D3 91 13 9D C0 12 02 E4 4C BB 6C 77

48 EE 6F 4B 9B 53 60 98 45 A5 28 65 8A 0B F8 39

73 D7 1A 44 13 B3 6A BB 61 44 AF 31 47 E7 87 C2

AE 7A A7 2C 3A D9 5C 2E 42 1A A6 78 FE 2C AD ED

39 3F FA D0 AD 3D D9 C5 3D 28 EF 3D 67 B1 E0 68

3F 58 A0 19 27 CC 27 C9 E8 D8 1E 7E EE 91 DD 13

B3 47 EF 57 1A CA FF 9A 60 E0 64 08 AA E2 92 D0}

condition:

any of them

}

{

meta:

description = “DDoS Misspelled Strings”

strings:

$STR1 = "Wating" wide ascii

$STR2 = "Reamin" wide ascii

$STR3 = "laptos" wide ascii

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and 2 of them

}

{

meta:

description = “DDoS Random URL Builder”

strings:

$randomUrlBuilder = { 83 EC 48 53 55 56 57 8B 3D ?? ?? ?? ?? 33 C0 C7 44 24 28 B4 6F 41 00 C7 44 24 2C B0 6F 41 00 C7 44 24 30 AC 6F 41 00 C7 44 24 34 A8 6F 41 00 C7 44 24 38 A4 6F 41 00 C7 44 24 3C A0 6F 41 00 C7 44 24 40 9C 6F 41 00 C7 44 24 44 94 6F 41 00 C7 44 24 48 8C 6F 41 00 C7 44 24 4C 88 6F 41 00 C7 44 24 50 80 6F 41 00 89 44 24 54 C7 44 24 10 7C 6F 41 00 C7 44 24 14 78 6F 41 00 C7 44 24 18 74 6F 41 00 C7 44 24 1C 70 6F 41 00 C7 44 24 20 6C 6F 41 00 89 44 24 24 FF D7 99 B9 0B 00 00 00 F7 F9 8B 74 94 28 BA 9C 6F 41 00 66 8B 06 66 3B 02 74 34 8B FE 83 C9 FF 33 C0 8B 54 24 60 F2 AE 8B 6C 24 5C A1 ?? ?? ?? ?? F7 D1 49 89 45 00 8B FE 33 C0 8D 5C 11 05 83 C9 FF 03 DD F2 AE F7 D1 49 8B FE 8B D1 EB 78 FF D7 99 B9 05 00 00 00 8B 6C 24 5C F7 F9 83 C9 FF 33 C0 8B 74 94 10 8B 54 24 60 8B FE F2 AE F7 D1 49 BF 60 6F 41 00 8B D9 83 C9 FF F2 AE F7 D1 8B C2 49 03 C3 8B FE 8D 5C 01 05 8B 0D ?? ?? ?? ?? 89 4D 00 83 C9 FF 33 C0 03 DD F2 AE F7 D1 49 8D 7C 2A 05 8B D1 C1 E9 02 F3 A5 8B CA 83 E1 03 F3 A4 BF 60 6F 41 00 83 C9

FF F2 AE F7 D1 49 BE 60 6F 41 00 8B D1 8B FE 83 C9 FF 33 C0 F2 AE F7 D1 49 8B FB 2B F9 8B CA 8B C1 C1 E9 02 F3 A5 8B C8 83 E1 03 F3 A4 8B 7C 24 60 8D 75 04 57 56 E8 ?? ?? ?? ?? 83 C4 08 C6 04 3E 2E 8B C5 C6 03 00 5F 5E 5D 5B 83 C4 48 C3 }

condition:

$randomUrlBuilder

}

Impact

A successful network intrusion can have severe impacts, particularly if the compromise becomes public and sensitive information is exposed. Possible impacts include:

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization's reputation.

Solution

Mitigation Strategies

Network administrators are encouraged to apply the following recommendations, which can prevent as many as 85 percent of targeted cyber intrusions. The mitigation strategies provided may seem like common sense. However, many organizations fail to use these basic security measures, leaving their systems open to compromise:

1. **Patch applications and operating systems** – Most attackers target vulnerable applications and operating systems. Ensuring that applications and operating systems are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker. Use best practices when updating software and patches by only downloading updates from authenticated vendor sites.
2. **Use application whitelisting** – Whitelisting is one of the best security strategies because it allows only specified programs to run while blocking all others, including malicious software.
3. **Restrict administrative privileges** – Threat actors are increasingly focused on gaining control of legitimate credentials, especially credentials associated with highly privileged accounts. Reduce privileges to only those needed for a user's duties. Separate administrators into privilege tiers with limited access to other tiers.
4. **Segment networks and segregate them into security zones** – Segment networks into logical enclaves and restrict host-to-host communications paths. This helps protect sensitive information and critical services, and limits damage from network perimeter breaches.
5. **Validate input** – Input validation is a method of sanitizing untrusted input provided by users of a web application. Implementing input validation can protect against the security flaws of web applications by significantly reducing the probability of successful exploitation. Types of attacks possibly averted include Structured Query Language (SQL) injection, cross-site scripting, and command injection.
6. **Use stringent file reputation settings** – Tune the file reputation systems of your anti-virus software to the most aggressive setting possible. Some anti-virus products can limit

execution to only the highest reputation files, stopping a wide range of untrustworthy code from gaining control.

7. **Understand firewalls** – Firewalls provide security to make your network less susceptible to attack. They can be configured to block data and applications from certain locations (IP whitelisting), while allowing relevant and necessary data through.

Response to Unauthorized Network Access

Enforce your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. Meanwhile, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact DHS or your local FBI office immediately. To report an intrusion and request resources for incident response or technical assistance, you are encouraged to contact DHS NCCIC (NCCICCustomerService@hq.dhs.gov or 888-282-0870), the FBI through a local field office, or the FBI's Cyber Division (CyWatch@fbi.gov or 855-292-3937).

Protect Against SQL Injection and Other Attacks on Web Services

To protect against code injections and other attacks, system operators should routinely evaluate known and published vulnerabilities, periodically perform software updates and technology refreshes, and audit external-facing systems for known web application vulnerabilities. They should also take the following steps to harden both web applications and the servers hosting them to reduce the risk of network intrusion via this vector.

- Use and configure available firewalls to block attacks.
- Take steps to secure Windows systems, such as installing and configuring Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and Microsoft AppLocker.
- Monitor and remove any unauthorized code present in any www directories.
- Disable, discontinue, or disallow the use of Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) as much as possible.
- Remove unnecessary HTTP verbs from web servers. Typical web servers and applications only require GET, POST, and HEAD.
- Where possible, minimize server fingerprinting by configuring web servers to avoid responding with banners identifying the server software and version number.
- Secure both the operating system and the application.
- Update and patch production servers regularly.
- Disable potentially harmful SQL-stored procedure calls.
- Sanitize and validate input to ensure that it is properly typed and does not contain escaped code.
- Consider using type-safe stored procedures and prepared statements.
- Audit transaction logs regularly for suspicious activity.
- Perform penetration testing on web services.
- Ensure error messages are generic and do not expose too much information.

Permissions, Privileges, and Access Controls

System operators should take the following steps to limit permissions, privileges, and access controls.

- Reduce privileges to only those needed for a user's duties.

- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
- Carefully consider the risks before granting administrative rights to users on their own machines.
- Scrub and verify all administrator accounts regularly.
- Configure Group Policy to restrict all users to only one login session, where possible.
- Enforce secure network authentication, where possible.
- Instruct administrators to use non-privileged accounts for standard functions such as web browsing or checking webmail.
- Segment networks into logical enclaves and restrict host-to-host communication paths. Containment provided by enclaving also makes incident cleanup significantly less costly.
- Configure firewalls to disallow Remote Desktop Protocol (RDP) traffic coming from outside of the network boundary, except for in specific configurations such as when tunneled through a secondary virtual private network (VPN) with lower privileges.
- Audit existing firewall rules and close all ports that are not explicitly needed for business. Specifically, carefully consider which ports should be connecting outbound versus inbound.
- Enforce a strict lockout policy for network users and closely monitor logs for failed login activity. Failed login activity can be indicative of failed intrusion activity.
- If remote access between zones is an unavoidable business need, log and monitor these connections closely.
- In environments with a high risk of interception or intrusion, organizations should consider supplementing password authentication with other forms of authentication such as challenge/response or multifactor authentication using biometric or physical tokens.

Logging Practices

System operators should follow these secure logging practices.

- Ensure event logging, including applications, events, login activities, and security attributes, is turned on or monitored for identification of security issues.
- Configure network logs to provide adequate information to assist in quickly developing an accurate determination of a security incident.
- Upgrade PowerShell to new versions with enhanced logging features and monitor the logs to detect usage of PowerShell commands, which are often malware-related.
- Secure logs in a centralized location and protect them from modification.
- Prepare an incident response plan that can be rapidly administered in case of a cyber intrusion.

References

- [1] IBM. Actor Lazarus Group – Blog Post by IBM X-Force Exchange.
- [2] AlienVault. Operation Blockbuster Unveils the Actors Behind the Sony Attacks.
- [3] Symantec. Destover: Destructive Malware has links back to attacks on South Korea.
- [4] Symantec. Duuzer back door Trojan targets South Korea to take over computers.
- [5] FireEye. Zero-Day HWP Exploit.
- [6] US-CERT. Alert (TA14-353A) Targeted Destructive Malware. Original Release Date: 12/19/2014 | Last revised: 9/30/2016

- [7] Novetta. Operation Blockbuster Destructive Malware Report.

Revisions

- June 13, 2017: Initial Release
- August 23, 2017: Updated YARA Rules and included MAR-10132963 (.pdf and .stix files)

This product is provided subject to this Notification and this Privacy & Use policy.

DECLARATION OF DANA BOWERS

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

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRIAN P. KEMP, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

DECLARATION OF DANA BOWERS

DANA BOWERS hereby declares as follows:

1. I am have been a Georgia voter since May 7, 2002 and am currently registered to vote at 3514 Debbie Ct. Duluth, GA 30097 I have been registered to vote at this address continuously since April 16, 2013.
2. When I have voted on Election Day, I have voted at Precinct 96 at 3180 Bunten Rd. Duluth, GA 30096 for 5 years, without a problem.
3. I am the Advocacy Coordinator in candidate Josh McCall's campaign for the the 9th Congressional District. As a part of my McCall campaign work, I have been active in voter protection, voter outreach and voter registration activities.

4. One of my responsibilities for the campaign is monitoring possible voting problems in the 9th Congressional District, which includes Hall County.
5. On approximately June 28, 2018 I received reports of a machine results tape in Hall County Precinct 10 that did not include the 9th Congressional District race in the May 22, 2018 primary election, which it should have, as well as other races (identified below). I received a photo of the key portion of the voting machine results tape (Exhibit 1) taken on election night by Kim Copeland, Chairman of the Hall County Democratic Party. I immediately undertook research on the discrepancy. That research is incomplete because Hall County has declined to fulfill my public records requests for information related to the discrepancy.
6. The photo of the results tape (Exhibit 1) shows that the following races were missing from the machine results tape in Hall County:

    - U.S. Representative, District 9 - REP
    - U.S. Representative, District 9 - DEM
    - State Senator, District 49 - REP
    - State Representative, District 30 - REP
    - State Representative, District 30 - DEM
    - District Attorney, Northeastern Circuit - REP
    - Solicitor General - R
    - County Commissioner P1 - R
    - County Commissioner P1 – D

7. I obtained additional photos of machine tapes (Exhibit 2) from Alana Watkins, Democratic Candidate for State Representative in District 30, whose race was missing from the tape. The particular tape in question was for machine serial number 291032 and was printed at 9:59 pm. This was approximately 3 hours after the closing of the polls; tapes are required to be printed upon the closing of the polls.
8. I also obtained Mr. Copeland's video recording of the Precinct 10 results tapes, that provided more data for comparison. The video shows that the pollworkers certified all results tapes on the door, including the tape from machine 291032 missing certain races.

   The video recording can be found at the following link: https://www.dropbox.com/s/ea0599yeo5kiy5u/Candler%20election%20tape.mp4
9. On June 29, 2018 requested public records related to this discrepancy from Hall County Elections. After repeated emails, meetings, phone conversations and visits to her office, the majority of my requests for such public records have not been honored. The denial of access to public records has curtailed my ability to assess the cause of the problems or recommend mitigation efforts to Candidate Josh McCall.

10. I attended the Hall County Board of Elections meeting on July 10, 2018 and presented my concerns. Other citizens presented similar concerns at the meeting. In response, Elections Director Lori Wurtz stated that there were "no discrepancies" and that the photo was not proof of a discrepancy. Ms. Wurtz did not provide any explanation for the missing races. The Board of Elections refused to discuss the issue and adjourned the meeting.

11. As noted above, I made repeated oral and formal written requests for the related public records without meaningful success. Hall County initially took the position that the public records at issue related to this litigation and were not to be shown to the public.

12. On July 13, 2018 the Hall County Board of Elections conducted a special meeting to go into executive session to discuss "threatened litigation," and public records request. I have not threatened Hall County with litigation nor am I aware of any threatened litigation. I attended the very short public portion of the meeting to attempt to again express concern not only about the discrepant machine tapes, and reporting delays, but also their refusal to honor public records requests for key election records.

13. I was met at the July 13, 2018 meeting by five armed security officers assigned to the meeting (there were approximately 4 members of the public in attendance). I felt intimidated by this show of force which I interpreted to communicate to me and other concerned citizens that we should not pursue questions on election irregularities.

14. At the July 13, 2018 meeting, citizens challenged the Board of Elections about the legitimacy of their planned closed door session. Nevertheless, the Board shut out the public, and did not accept public comment before going into closed session.

15. Mr. Tom Smiley, Chairman of the Board of Elections, reported to me after the meeting that the Board decided in their closed door session that they would honor my public records request because I was not involved in the Curling v Kemp litigation, but would not honor requests from people associated with this lawsuit. However, to date, the County has only permitted me to examine a small portion of the records I requested.

16. I am concerned that by filing this affidavit, I will be retaliated against by the Hall County Board of Elections for involvement in the lawsuit, and the McCall campaign will continue be denied access to important public records.

17. On July 13, 2018 I was permitted to review the county's paper copy of the machine results tape from Precinct 10. Ms. Wurtz stated that they do not collect the tapes on the precinct doors and this was the county's copy printed at the same time. The county's copy contained vote tallies for the races missing from the tape copy on the door.
18. I note that, on the May 22, 2018 election night, Hall County results were delayed and not reported by media until after 11:30pm.
19. Because my public records request have been denied by Hall County, I have been unable to confirm reports of election night machine malfunctions that contributed to the late results reporting, although the late printing times for the machine tapes in Precint 10 indicate an unusual condition that should be thoroughly investigated.
20. I am aware that even if I have access to the public records, I will be unable to confirm that the results recorded reflect voters' votes on the unaudtiable touchscreen machines. I will be unable to confirm whether the missing races were on the electronic ballot on the problem machine because there is no paper record.
21. I have talked with voting system experts and read the research to understand that there is no way to audit whether the votes that were reported in the official results were actually cast by voters on the

touchscreen machines. However, I want to review and compare the records of this discrepancy.

22. I was told by Ms. Wurtz and Mr. Smiley that the likely cause for the missing races is that the problem machine tape may have failed to engage and print a portion of the results. Even if this speculation is accurate, there appears to be no way to verify whether that is sole problem and what impact it had, nor does it address why the results tapes were late in being printed, nor why they were certified by poll workers as accurate, when they were missing 9 races.

23. As of the date of this declaration, weeks after my repeated requests, Hall County has not yet permitted me to review public records related to the reported voting machine closing problems, results printing discrepancies, results reporting delays, and system logs for the machines.

24. On July 24, 2018 I voted in Gwinnett County precinct 100 (and report on discrepancies in my voter records below), and observed a voting machine discrepancy of concern to me.

25. When I was in the polling place, I noticed that one DRE voting machine (serial number 291429) was marked “Do Not Touch” and was not in service. I inquired about the machine and was told by Ms.

Williams, a poll worker, that the out-of-service machine "froze a few times" earlier in the day, and the poll manager made the decision to discontinue its use for the remainder of the election. I asked Ms. Williams if voters had been casting votes on the out-of-service machine before it appeared to malfunction. Ms. Williams confirmed that, yes, the out-of-service machine had been in use and ballots had been cast on it for approximately "an hour to an hour and a half" after the polling location, Gwinnett 100, had opened at 7am. Ms. Williams told me of one voter who attempted to use the machine when it froze up on the language selection screen.

26. Poll Manager Denise Sullivan, however, told me that voters had *not* cast votes on that machine. I have no way of knowing which story is accurate as to whether voters cast votes on the machine.

27. I asked whether the voter who experienced the frozen machine at the language selection screen had been able to cast a ballot and Ms. Sullivan told me that the voter had been given a provisional ballot to complete. I could not learn whether there was an attempt made to determine if this voter had successfully cast a vote on the DRE voting machine in addition to his provisional ballot.

28. If the machine was not functioning, I do not know why this voter would have been given a provisional ballot instead of being instructed to cast a vote on another machine without the necessity of checking his eligibility through the provisional process. I am concerned about the process of forcing voters to use provisional ballots when machines do not accept their vote. Provisional ballot credentials are time consuming to complete and therefore discourage some voters.

29. After the closing of the polls, I overhead the pollworkers talking about two machines for which the tabulations were not reconciling. I became curious about what the ballot and voter certificate reconciliation on the precinct recap sheet would show. Therefore, I asked Poll Manager Sullivan to see the polling place recap sheets, which I believe are public records. I wanted to see the discrepancy for myself, but I was denied access.

30. After the closing at the polls at 7pm, I watched carefully as poll workers attempted to print the closing tape on the out-of-service machine. Poll workers appeared to attempt at least four times to print the results tape. I stayed inside the polling place to watch the shutdown process which was being delayed by the problem machine.

31. I then went outside the polling place with Ms. Sullivan and took photographs of the DRE machine results tapes including machine number 192429 after they were posted on the door at approximately 8:40pm. I noticed that the results tape for this DRE machine showed no votes tallied on the machine and the results tape was attached to a "Zero tape" (used at opening of the polls to purportedly show that no votes are stored in memory). Both opening zero report and the closing results tape displayed printing times of 7:42 a.m. with no votes recorded for any candidate. (Exhibit 3)

32. Given that the tape was printed from a machine that had reportedly been used to record votes that day, and was printed well after the polls were closed, I was puzzled to see a 7:42 am time stamp, no votes cast, and the "Zero report" also attached to the results tape. The printing time of 7:42 am was also concerning as it would have been 42 minutes after the polls were open and over 11 hours before the polls were closed. Machine reports are supposed to be printed before the 7 am opening and immediately after the 7pm close.

33. Other machine results tapes that I recorded posted on the door showed print times of 7:36 pm and 7:29pm, which times are consistent with the time of day I observed the printing of the results tapes.

34. I am gravely concerned about the integrity of the upcoming election based my personal observations of DRE machine malfunctions in recent elections.

ELECTRONIC POLLBOOK AND

VOTER REGISTRATION DISCREPANCIES

35. Based on my awareness of widespread problems with wrong ballot issuance at polling places in the May 22, 2018 primary, I decided to verify my own voter registration records before voting on July 24, 2018. I checked my voter registration and polling place location on the My Voter Page on the Secretary of State's website (https://www.mvp.sos.ga.gov/MVP/mvp.do), and saw that my precinct number had apparently changed to Precinct 100, although I had not received a notice of such change.

36. My precinct has long been precinct 96, but I assumed the precinct assignments had changed and were authorized.

37. I went to Precinct 100 at 54 Buford Highway, Suwanee, Georgia, at approximately 6:20 pm and completed the voter application form in order to vote.

38. I presented my driver's license to the pollworker whose first name is Christine. I do not know her last name. She located my name in the

electronic pollbook and told me that I was in the wrong precinct location, and that I was supposed to vote in Precinct 96, not 100. I explained that I had checked my registration on the Secretary of State website that morning and that my assigned precinct was 100 at the Suwanee polling place.

39. Another pollworker, Carolyn Williams told me, "Don't worry Ms. Bowers, this has been happening all day," and went on to tell me that she was aware of approximately 50 voters who had been assigned the wrong precinct.

40. Pollworker Christine suggested that I vote a provisional ballot given that there was not time to get to precinct 96 by 7 pm when the polls would close. She assured me that the provisional ballot would be counted.

41. I completed my provisional ballot information, marked the paper ballot, and cast it, enclosed in an envelope, and in the large locked black box I had been directed to.

42. At 8:55pm that evening, I checked my voter registration page again on the My Voter Page on the Secretary of State website and captured screenshots (Exhibit 4) which showed the same Precinct 100 assignment as it had that morning (Election Day).

43. Several days later, at 7:24pm on July 29, 2018, I checked My Voter Page again and my precinct assignment displayed Precinct 096, having been changed back to my original precinct 96. (Exhibit 5). I had not made any changes to my voter registration nor requested a correction.

44. Precincts 96 and 100 are not identical precincts in the same governmental jurisdictions. The misassignment can have the effect of disenfranchising voters by giving them the wrong ballots or forcing them to vote provisional ballots because they are not on the electronic pollbook in the precinct stated on the SOS voter registration website. I am concerned that a wrong assignment will also occur in the November election and I will be disenfranchised. I am also concerned about the impact on election integrity overall, as these malfunctions in the pollbooks or voter records happen to other voters.

45. In my work to protect 9th Congressional District voters' ability to vote in the correct races and avoid disenfrachinsement in the upcoming November election, I have undertaken research work using the voter registration records. I personally researched dozens of registration records for voters who were allegedly assigned to the wrong Georgia House District and allegedly received incorrect ballots in Habersham,

Banks, Stephens, Franklin and Jackson Counties in the May 22, 2018 primary, based on voter specific information disclosed in the election contest pending in Fulton Superior Court (Fulton County Superior Court (2018CV306197)). These counties are in the 9th Congressional District so they are of primary interest.

46. I used information on from Vote Builder, the Democratic Party's voter history database, fed by the Secretary of State's official database, and designed specifically for use by candidates and campaign staff, and My Voter Page on the Secretary of State's website to compare House District assignments on the two records to the information disclosed in the election contest complaint. I personally reviewed numerous discrepancies between the various voter assignment records including the House District Maps.

47. I am concerned about discrepancies in the pollbooks and voter registration files in anticipation of the November election. I do not believe that provisional ballots are an adequate remedy for inaccurate voter rolls. I recognize that provisional ballots can unintentionally disenfranchise voters voting in the wrong precinct, as candidates in their home precinct may not be on the provisional ballot voted in a different precinct.

48. Because of the numerous and widespread voter registration discrepancies I am personally aware of, I am concerned about my own vote, the votes for Mr. McCall in the 9th Congressional District, and more generally for the voters of the state in the upcoming election.

49. If Georgia does not adopt paper ballots in the polling places for the November 2018 election, I plan to vote by mail-in paper ballot. I will accept the inconvenience of the absentee ballot application and voting process where I must vote in advance so that I may vote a verifiable ballot. In order to cast a secure ballot, I will have to give up my preference of voting in my home precinct on Election Day when all last minute campaign information will be available.

50. I will personally launch activist efforts to encourage voters to request a mail-in absentee ballot, so that their votes can be verified and recounted if necessary, even if it adds expense and inconvenience to the voting process.

51. I am a member of Coalition for Good Governance.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, August 3, 2018.

_____

Dana Bowers

EXHIBIT 1

TIMES COUNTED 75
TIMES BLANK VOTED 15
C. EATON (I) 60
****
PSC Eaton- D
RACE # 91 PARTY:DEM
RUNNING 3
TO VOTE FOR 1

TIMES COUNTED 21
TIMES BLANK VOTED 4
L. MILLER 11
J. NOEL 3
J. C. WHITE 3
****
PSC Pridemore- R
RACE # 95 PARTY:REP
RUNNING 2
TO VOTE FOR 1

TIMES COUNTED 75
TIMES BLANK VOTED 11
J. HITCHINS III 30
T. PRIDEMORE (I) 34
****
PSC Pridemore- D
RACE # 96 PARTY:DEM
RUNNING 2
TO VOTE FOR 1

TIMES COUNTED 21
TIMES BLANK VOTED
RACE # 476 PARTY:REP
RUNNING 1
TO VOTE FOR 1

TIMES COUNTED 74
TIMES BLANK VOTED 9
B. THOMPSON (I) 65
****
BOE At Large - D
RACE # 477 PARTY:DEM
RUNNING 1
TO VOTE FOR 1

TIMES COUNTED 19
TIMES BLANK VOTED 4
S. LOPEZ 15
****
BOE 1 - R
RACE # 479 PARTY:REP
RUNNING 1

DECLARATION

EXHIBIT 2

Hall County
State of
Georgia Primary and
Nonpartisan General
Election
May 22, 2018
DATE: May-22-2018
POLL CTR: 180
10-Candler
MACHINE ID: 3
VERSION: 1 COPY: 0
COUNT: 0 SIZE: 32M
ACCU-VOTE RELEASE: 4.5.2
REPORT: US 1.14.7

TIME: 21:59 05/22/2018
MACHINE SERIAL: 291032
PUBLIC COUNTER: 98
SYSTEM COUNTER: 1499

** PRECINCT: 120 **
10-Candler

BALLOTS CAST

BALLOT	QUANTITY
1	2
4 REP	11
5 DEM	11
6 REP	42
7 DEM	8
15 REP	1
16 DEM	2
21 REP	21
22 REP	0
TOTAL	98

BALLOTS CAST SUMMARY

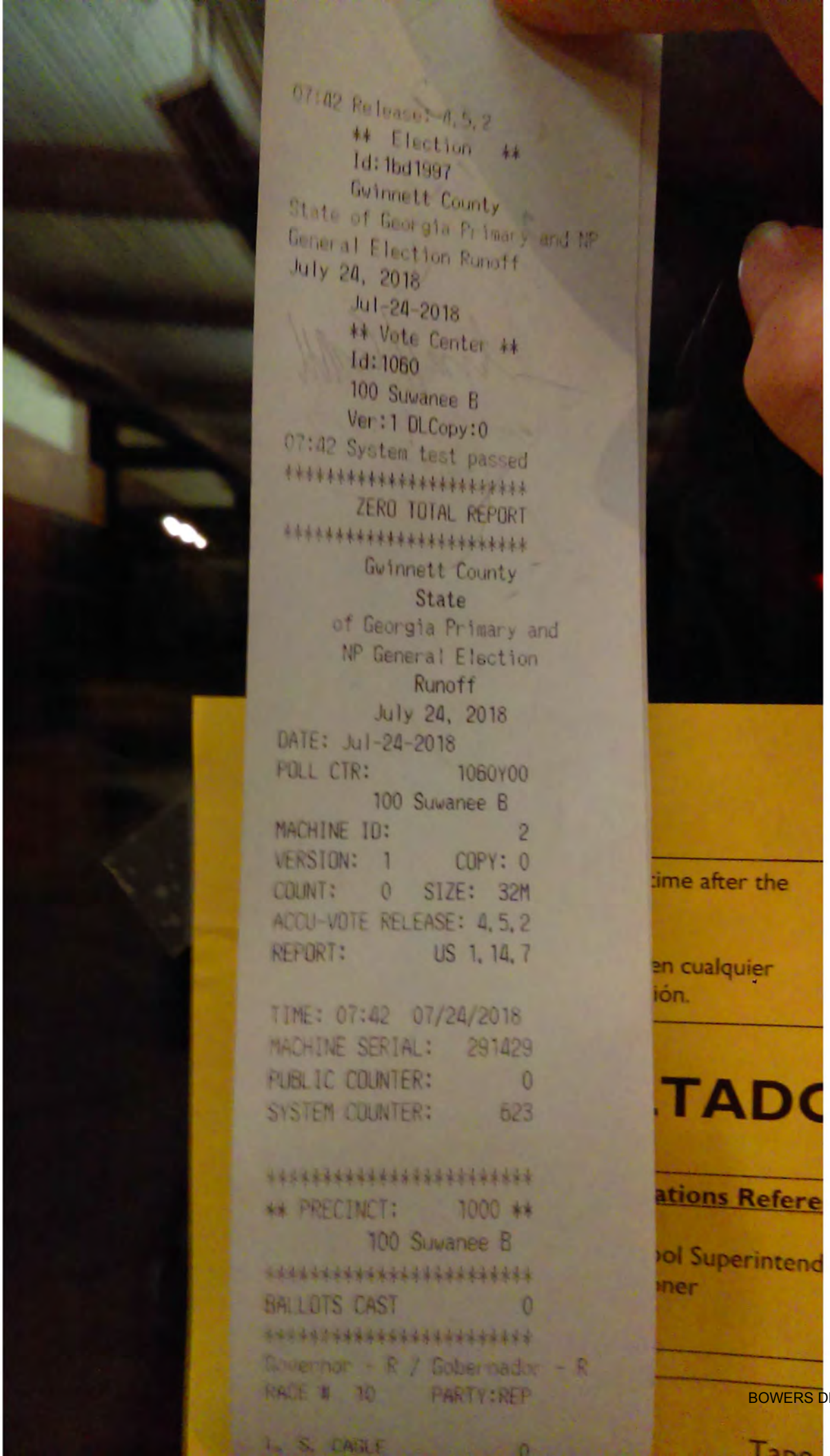
BLANK VOTED	0
UNDERVOTED	0
WRITE-IN	3

Governor - R
RACE # 50 PARTY:REP
RUNNING 7
TO VOTE FOR 1

# TIMES COUNTED	75
# TIMES BLANK VOTED	0
L.S. CAGLE	40
E. HAYES	1
H. HILL	10
B. KEMP	11
C. TIPPINS	9

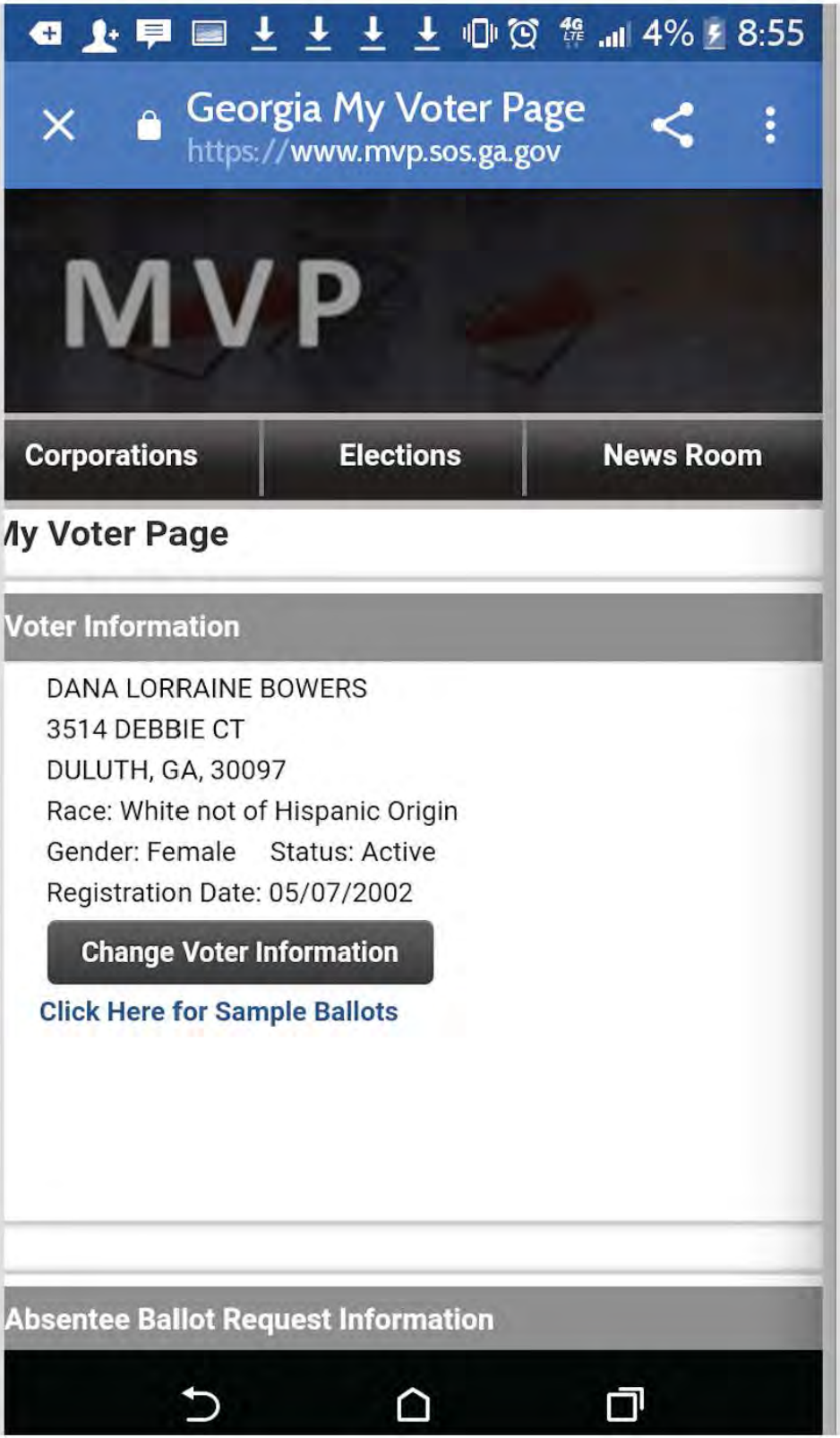
BOWERS DECLARATION

EXHIBIT 3



BOWERS DECLARATION

EXHIBIT 4


4% 8:55
Georgia My Voter Page
https://www.mvp.sos.ga.gov
MVP
Corporations
Elections
News Room
My Voter Page
Voter Information
DANA LORRAINE BOWERS
3514 DEBBIE CT
DULUTH, GA, 30097
Race: White not of Hispanic Origin
Gender: Female Status: Active
Registration Date: 05/07/2002
Change Voter Information
Click Here for Sample Ballots
Absentee Ballot Request Information

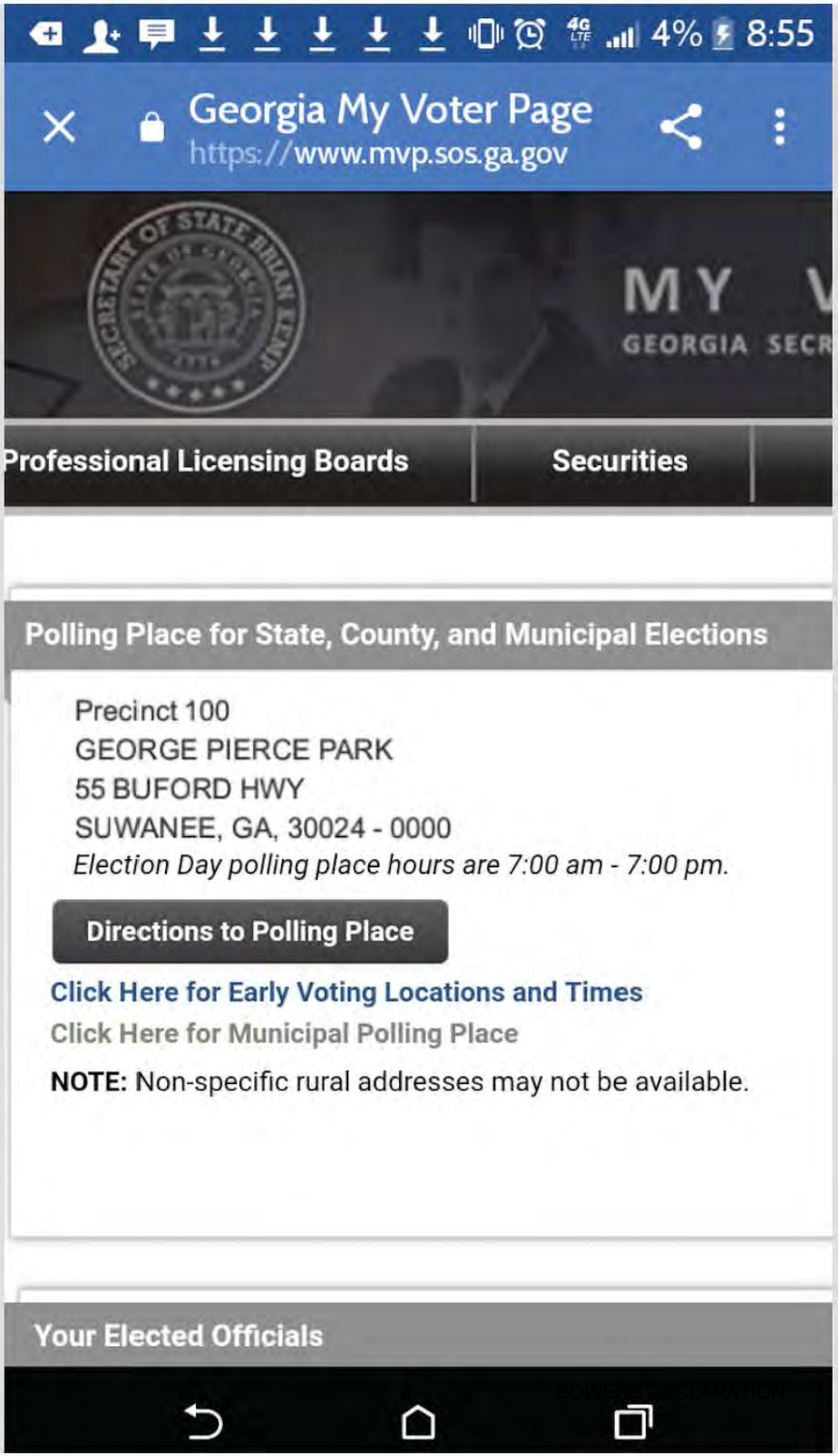
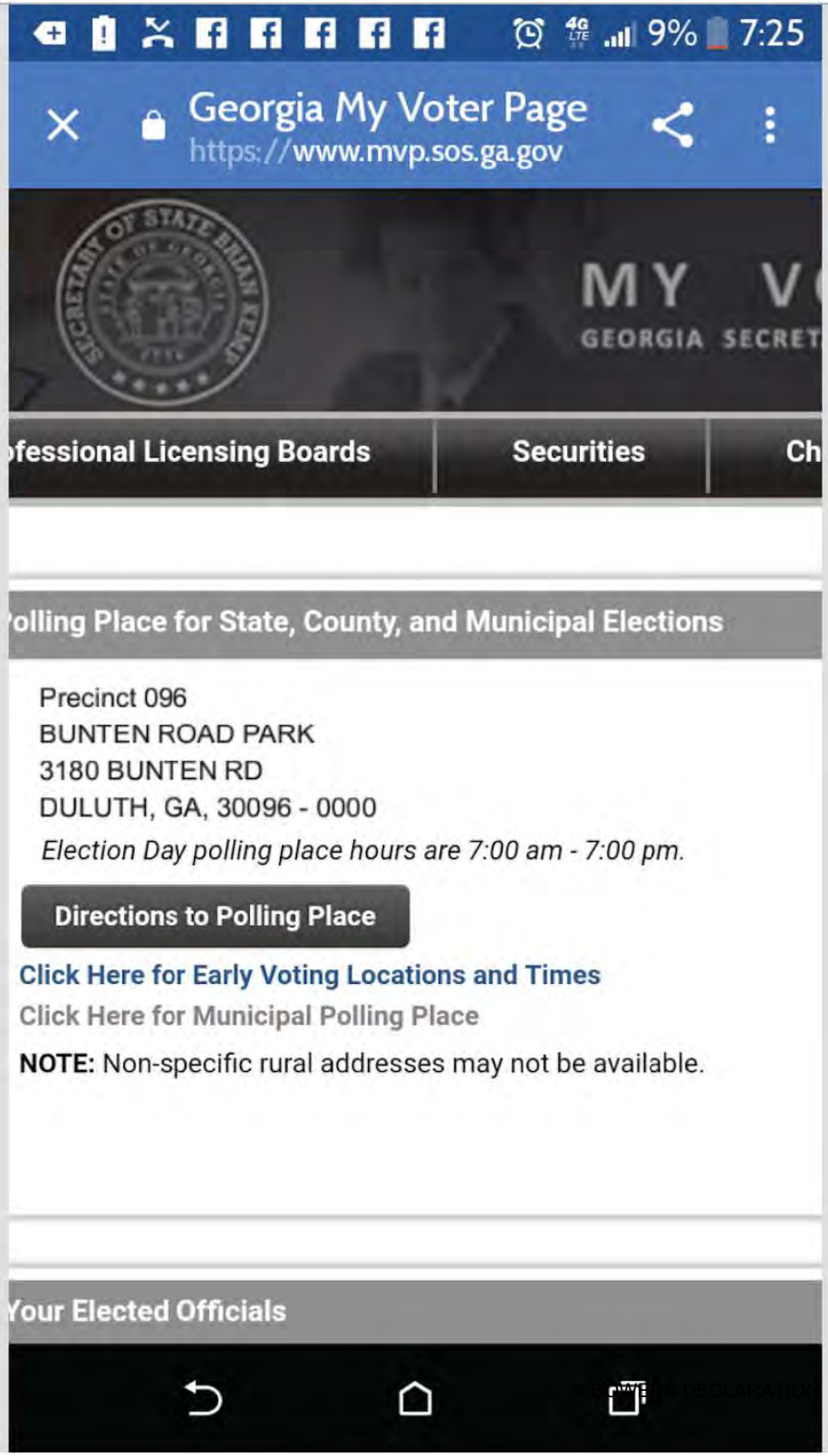

4% 8:55
Georgia My Voter Page
https://www.mvp.sos.ga.gov
GEORGIA SECR
Professional Licensing Boards
Securities
Polling Place for State, County, and Municipal Elections
Precinct 100
GEORGE PIERCE PARK
55 BUFORD HWY
SUWANEE, GA, 30024 - 0000
Election Day polling place hours are 7:00 am - 7:00 pm.
Directions to Polling Place
Click Here for Early Voting Locations and Times
Click Here for Municipal Polling Place
NOTE: Non-specific rural addresses may not be available.
Your Elected Officials

EXHIBIT 5

9% 7:24
Georgia My Voter Page
https://www.mvp.sos.ga.gov
MVP
Corporations
Elections
News Roon
My Voter Page
Voter Information
DANA LORRAINE BOWERS
3514 DEBBIE CT
DULUTH, GA, 30097
Race: White not of Hispanic Origin
Gender: Female Status: Active
Registration Date: 05/07/2002
Change Voter Information
Click Here for Sample Ballots
Absentee Ballot Request Information


9% 7:25
Georgia My Voter Page
https://www.mvp.sos.ga.gov
MY V
GEORGIA SECRET
ofessional Licensing Boards
Securities
Ch
olling Place for State, County, and Municipal Elections
Precinct 096
BUNTEN ROAD PARK
3180 BUNTEN RD
DULUTH, GA, 30096 - 0000
Election Day polling place hours are 7:00 am - 7:00 pm.
Directions to Polling Place
Click Here for Early Voting Locations and Times
Click Here for Municipal Polling Place
NOTE: Non-specific rural addresses may not be available.
Your Elected Officials

DECLARATION OF BRUCE P. BROWN

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

DONNA CURLING, ET AL., **Plaintiffs** **, v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF BRUCE P. BROWN

BRUCE P. BROWN hereby declares as follows:

1. I am an attorney licensed to practice law in Georgia. I am one of the attorneys representing Plaintiffs in this action.

2. Attached hereto as Exhibit 1 is a true and correct copy of a letter that I sent to Defendants' counsel Governor Roy Barnes and John Salter dated July 26, 2018. This letter includes as an exhibit my April 16, 2018 letter to Governor Barnes and Mr. Salter.

3. Attached hereto as Exhibit 2 is a true and correct copy of an August 1, 2018 memorandum from Chris Harvey, State of Georgia's Elections Division Director, to County Election Officials and County Registrars.

4. In accordance with 28 U.S.C. § 1746, I pledge under penalty of perjury that the foregoing is true and correct.

Executed on this date, August 3, 2018.

Bruce P. Brown

EXHIBIT 1

Bruce P.
Brown
Law

July 26, 2018

By Email

Roy E. Barnes
John F. Salter
Barnes Law Group, LLC
31 Atlanta Street
Marietta, GA 30060

Re: *Curling, et al. v. Kemp, et al.*, No. 17-CV-02989-AT (N.D. Ga.)

Dear Governor Barnes and Mr. Salter:

We want to bring to your attention todays' news that House Intelligence Committee Chairman Devin Nunes has joined many federal officials and agencies concerned with national security to call for a ban on electronic voting.[1] Similarly, in March, DHS Secretary Nielsen labeled such systems "a national security concern."[2]

Given the escalating threats of election manipulation in voting systems that cannot be audited, we again urge the Secretary and the State Board to adopt paper ballots for the November election as specified in our letter of April 16, 2018, which is attached. Further, given the widespread reports of voter roll discrepancies in this past Tuesday's run-off election, and in the May 22, 2018 primary election, we again implore Secretary Kemp to immediately initiate a thorough voter registration record audit to ensure that all eligible voters will be able to vote in their proper districts without administrative delays or excessive use of provisional ballots.

If you have questions about the details of our proposals as detailed in the attached letter, please let us know.

Sincerely,

Bruce P. Brown

cc: Cary Ichter
Robert A. McGuire, III
William Brent Ney
Marilyn R. Marks

[1] http://thehill.com/hilltv/rising/398949-house-intel-chair-calls-for-ban-on-electronic-voting-systems.
[2] https://www.reuters.com/article/us-usa-trump-russia-security/inability-to-audit-u-s-elections-a-national-security-concern-homeland-chief-idUSKBN1GX200.

404-881-0700 | 1123 Zonolite Road NE, Suite #6, Atlanta, GA 30306
bbrown@brucepbrownlaw.com | www.brucepbrownlaw.com

cc: (continued)

David D. Cross
Halsey G. Knapp, Jr.

Bruce P.
Brown
Law

April 16, 2018

By Email

Roy E. Barnes
John F. Salter
Barnes Law Group, LLC
31 Atlanta Street
Marietta, GA 30060

Re: *Curling, et al. v. Kemp, et al.*, No. 17-CV-02989-AT (N.D. Ga.)

Dear Governor Barnes and Mr. Salter:

Together with Robert McGuire, Cary Ichter and William Ney, I represent the Coalition for Good Governance, Laura Digges, William Digges III, Ricardo Davis and Megan Missett ("the Coalition Plaintiffs") in the above-styled litigation. The purpose of this letter is to make another urgent demand upon your clients Brian P. Kemp, the Secretary of State of Georgia, and Georgia State Election Board Members David J. Worley, Rebecca N. Sullivan, Ralph F. Simpson, and Seth Harp (the "State Election Board"). Specifically, the Coalition Plaintiffs demand that Secretary Kemp and the Election Board exercise their power, authority and responsibilities under Georgia law and the United States Constitution to conduct the upcoming 2018 elections involving federal and state offices, specifically the May 22, 2018 primary election, any resulting July 24, 2018 runoff elections, and the November 6, 2018 elections, and any special elections, using hand-marked paper ballots in lieu of the Direct Recording Electronic ("DRE") machines.

The unreliability, unverifiability and vulnerability of Georgia's DRE systems is the subject of daily local and national news reports and continuing warnings from federal agencies, such as the Department of Homeland Security, the Election Assistance Commission, and the Federal Bureau of Investigation. As recently as last month, the U.S. Senate Select Committee on Intelligence renewed its warnings concerning the unacceptable risks of paperless electronic voting systems of the type Georgia uses. We need not repeat here the many warnings from the authorities and private sector experts concerning the urgent need to decommission Georgia's DRE machines in favor of paper ballots.

As the Coalition Plaintiffs have explained in detail in their Proposed Third Amended Complaint, filed on April 4, 2018, because Georgia's DRE touchscreen voting machines are insecure, lack a voter verified paper audit capacity, fail to meet minimum statutory requirements, and deprive in-person voters of the ability to cast a secret ballot

as guaranteed by Ga. Const. Art. II, § 1, ¶ 1, requiring in-person voters to use those machines violates the voters' constitutional rights to have their votes recorded in a fair, precise, verifiable, and anonymous manner, and to have their votes counted and reported in an accurate, auditable, legal, and transparent process.

"The right to vote freely for the candidate of one's choice is of the essence of a democratic society, and any restrictions on that right strike at the heart of representative government." *Reynolds v. Sims*, 377 U.S. 533, 555 (1964). The secret ballot—"the hard-won right to vote one's conscience without fear of retaliation"—is a cornerstone of this right to freely vote for one's electoral choices. *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 343 (1995).

In their Proposed Third Amended Complaint, the Coalition Plaintiffs have explained in detail the factual and legal basis for their claims for injunctive relief. The Coalition Plaintiffs again urge the Secretary and the State Election Board to take immediate remedial action to protect the 2018 elections by requiring the statewide use of hand-marked paper ballots. As explained below, the Secretary and the State Election Board have the statutory authority to take this remedial action, and have feasible, economic and practical means for replacing DREs machines with paper-ballot voting immediately.

The Coalition and its supporters have made these or similar demands repeatedly over the past eleven months, and they are made again here with renewed urgency.

A. Statutory Authority

The Secretary stated in his Brief Supporting the State's Motion to Dismiss that he has the "discretionary authority to choose voting equipment for counties." (Doc. 83-1 at 20, 21). Indeed, the Secretary and the State Board have selected, and the State has provided, both DRE voting machines and paper ballot optical scanners for every county in Georgia.

Paper ballots have been an authorized form of voting under Georgia law continuously for over 240 years. (Article IX Georgia Constitution of 1777). Paperless mechanical lever voting machines were first permitted in approximately 1930 and optical scanners were authorized for the counting of paper ballots by 1981. (*See* O.C.G.A. §§ 21-2-280). DRE machines were first permitted in 2002. Ga. L. 2002, p. 598; Ga. L. 2003, p. 517. None of these laws authorizing mechanical or electronic voting systems, however, required their use or supplanted the authority to use hand-counted or electronically counted paper ballots.[1]

[1] Indeed, numerous Georgia statutes authorize, require or contemplate the use of paper ballots today. *See, e.g.*, O.C.G.A. § 21-2-280; § 21-2-281;§ 21-2-366; and § 21-2-4-483.

O.C.G.A. § 21-2-379.3 permitted Georgia's first use of DRE voting systems in 2002 and required that the Secretary of State provide DRE equipment to all counties, after funds were appropriated by the General Assembly. The law, however, does not mandate their use. In fact, the State provided both DREs and optical scanning equipment for paper ballots. Further, counties retain the statutory authority to use optical scanning equipment to scan and count paper ballots, and absentee mail-in and provisional ballots.

In addition, under O.C.G.A. § 21-2-379.2, the Secretary has the authority to revoke his approval of a DRE voting system if he re-examines the system and determines that it "can no longer be safely or accurately used by electors at primaries or elections . . . because of any problem concerning its ability to accurately record or tabulate votes." An examination of the evidence and undisputed academic research would require such a finding and a wholesale revocation of Georgia's DREs. However, given the underlying statutory authority to use paper ballots (either hand-counted or counted by optical scan equipment), and the absence of any state law requiring use of DREs, the replacement of the DREs in lieu of paper ballots does not require the Secretary to invoke O.C.G.A. § 21-2-379.2.

It is true that on April 17, 2005, the State Election Board promulgated Rule 183-1-12-.01 which requires the use of DREs for in-person voting for county, state and federal elections. In doing so, the State Election Board clearly exceeded its authority under Georgia law, which does not require DREs to be used and explicitly allows the use of paper ballots. The General Assembly has charged the State Election Board to promulgate rules to ensure the "legality and purity in all primaries and elections." O.C.G.A. § 21-2-31. Given the overwhelming evidence that the DREs are not reliable or secure, and cannot comply with the operational and security requirements of O.C.G.A. § 21-2-379.1 *et seq.*,[2] the Election Board has the statutory duty to repeal Rule 183-1-12-.01 immediately, and can do so on an emergency basis. In any event, the Board's Rule provides no defense to the mandates of state and federal law.

In sum, the Secretary and the State Election Board have the clear statutory authority and duty to discontinue the DRE voting systems and to order the use of hand-marked paper ballots.

B. Practical and Feasible Means for Using Paper Ballots

[2] *See* Second Amended Complaint ¶¶ 110-121 for details.

There are at least three feasible methods of conducting paper ballot elections in 2018. Each county board of elections should be permitted to choose the paper ballot system that best suits local needs for conducting a secure election in their jurisdiction.

1. Precinct optical scanning of paper ballots

   (i) Method: voters hand-mark paper ballots and insert the ballots into the Accu-Vote OS optical scanners of the type currently in use for paper ballots. Votes are tabulated by the optical scanners at the polling location after polls close, and the tabulated results are posted on the door of the polling place. Then, the tabulated results are securely transported from the polling location to the county election office by hand delivery of the memory cards and results tapes along with all balloting materials. Unofficial results can be immediately emailed from the polling place to the county election office using digital photos of the results tapes, while county officials await the election night hand delivery of the secured original records.

   (ii) Statutory authority: O.C.G.A. §21-2-483(a). This is the best overall solution, and is the method that Georgia used prior to the 2002 implementation of the DREs. Specific procedures are provided in Title 21, Chapter 2, Article 11 Part 5, and security requirements can be updated and strengthened by promulgation of Election Board Rules.

2. Central count optical scanning of paper ballots

   (i) Method: voters hand-mark paper ballots and cast them into traditional secured ballot boxes at the polling locations. After polls close, the locked boxes are securely transported to the county elections office for ballot counting and reporting using the currently-owned and state-approved Accu-Vote OS scanners. Vote totals for each precinct and the county would be consolidated by the county Elections Department and reported to the public and the Secretary of State using the current GEMS election management system. Although "precinct scan" (described in 1 above) is preferable from a security perspective, the central count method may be temporarily attractive to counties that are concerned about training enough precinct workers to use one scanner

in each polling place.

(ii) Statutory authority: O.C.G.A.§ 21-2-483(a). Specific procedures are provided in Title 21, Chapter 2, Article 11 Part 5, and security requirements can be updated and strengthened by promulgation of Election Board Rules

3. Traditional hand-counted paper ballots

(i) Method: Voters hand-mark paper ballots, casting them in a traditional secured ballot box. The ballots are manually counted by teams of poll workers in the neighborhood precincts, typically within two hours of the closing of the polls. Unofficial results could be immediately transmitted by an emailed digital photo of the precinct tally sheets, to be immediately followed by Election Night hand delivery of the secured original tally sheets, ballots, and election records to the county Election Board. This is an easily implementable alternative, particularly for the May and July primaries in smaller population counties.

(ii) Statutory authority: O.C.G.A.§21-2-280. Numerous Georgia municipalities employ hand counted paper ballots routinely for all municipal elections with detailed procedures are provided by Title 21, Chapter 2, Article 11, Part 2.

In addition, in jurisdictions where optical scan equipment is used, and given the well-documented security risks associated with the Accu-Vote OS and GEMS election management system, it is imperative that, prior to programming for the 2018 elections, such components be thoroughly disinfected and determined to be free from any unauthorized software code. Trusted build copies of the approved software must be reinstalled on all machines after the machines have been fully examined or replaced. It is also imperative that robust post-election audits of the unofficial results be completed before the election results are certified.

The State has the equipment, supplies, software licenses and know-how necessary for all of these three alternatives. The paper ballots needed for these methods are already required to be printed for each precinct for use as mail-in ballots and provisional ballots. The counties merely need to increase the number of paper ballots ordered. A larger paper ballot print order will be a minimal cost, particularly when

compared to the cost of moving, storing, securing and setting up and taking down the DRE equipment.

As for the scanning equipment: the state owns approximately 1,000 Accu-Vote OS optical scanners used for counting mail-in and provisional ballots. The number of additional scanners needed, if any, will depend on which of the three methods various counties select. If additional scanners are required, other states and vendors have hundreds of surplus Accu-Vote OS machines that can be borrowed or rented inexpensively. Georgia already licenses and uses the software necessary for deployment of either of the optical scan methods, and election personnel in the county offices are already trained on the necessary equipment.

C. Sufficient Time Before Elections to Address the Problems

As you know, over the past eleven months, the Coalition Plaintiffs and other Coalition members have initiated numerous requests to Secretary Kemp and State Election Board Members to abandon the non-compliant DRE system and convert to paper ballots to ensure the security of Georgia's elections.[3]

Though these warnings and requests have not been heeded, there is still enough time to implement reasonable interim remedies. Virginia was faced with a similar election security issue in 2017. On September 8, 2017, Virginia's State Board of Elections decertified all DREs in the state because of concerns about the integrity of DRE voting systems.[4] Within two months, on November 7, 2017, twenty-two Virginia

---

[3]Prior notices and demands include the following: May, 2017 Change.org citizens petition to use paper ballots for the June 20, 2017 6th Congressional District runoff election (see emails directed to T. Fleming in Secretary of State' Office); May 10, 2017 Georgia voters' request that Secretary Kemp re-examine the DRE voting system under the provisions of O.C.G.A. § 21-2-379.2, with technical documentation supporting the necessity of halting the use of the DRE system (see May 10, 2017 email to T. Fleming and W. Harvey of SOS office); May 17, 2017 Georgia voters' follow up request for re-examination of DRE voting system with additional supporting technical documentation of inadequate system security (see May 17, 2017 email to T. Fleming); May 19 and June 2, 2017 Georgia voters' additional follow-up requests for response on DRE system re-examination prior to June 20, 2017 election (see emails to T. Fleming); May 25, 2017 complaint and motion for temporary restraining order to prohibit the use of the DRE voting system and to require use of paper ballots in the June 20, 2107 runoff election (Fulton County Superior Court, Case No. 2017CV290630); July 3, 2017 litigation to challenge the use of DRE voting systems in Georgia (N.D. Ga., Case No. 17-cv-02989).

[4]https://www.elections.virginia.gov/Files/Media/Agendas/2017/SBEResolutiondecertifyingDREs09-08-17.pdf

counties had immediately and successfully converted to hand-marked paper ballots. In the case of Georgia, Coalition's demands alone have been outstanding for eleven months, giving officials more than adequate time to prepare for hand-marked paper ballot elections. Additionally, officials in the Secretary of State's office have acknowledged the compromised nature of the voting system since its reporting of the August 24, 2016 breach at Center for Election Systems, and no material action has been taken to mitigate the impact of the security failures on voting system components.

Though the above methods cure the constitutional and statutory infirmities that plague the current system, and would greatly enhance voter confidence, the State should consider in due course the best long-term hand-marked paper ballot technology. Temporarily using the currently owned Accu-Vote OS paper ballot system, and hand counts for smaller counties, will permit a more deliberate and phased-in adoption and implementation of a new paper ballot voting system, without undue time pressures driven by the urgent need to decommission the DRE units.

D. Audit of Voter Registration Database

It is undisputed that the State's entire voter registration database including Personally Identifiable Information ("PII") for over 6.5 million voters was unprotected and available on the Center for Election System server to anyone with an internet connection from at least August 24, 2016 until at least March 3, 2017. Additionally, on April 15, 2017, equipment and memory cards containing the entire state voter registration database, also including PII, was stolen and not recovered. Such exposure permitted almost unlimited opportunities for malicious actors to alter voters' registrations including eligibility for voting in certain contests. Voters whose data was disclosed have not been notified of this inappropriate disclosure despite the legal requirement to do so under O.C.G.A § 10-1-912. *See* Second Amended Complaint ¶¶ 146-153.

Further, Fulton County officials have acknowledged that there are "glitches" in the voter registration database programs that can cause voters to be disenfranchised, such as Fulton voter Brian Blosser. *See* Proposed Third Amended Complaint ¶ 152.

The November 6, 2018 general election is the first statewide general election scheduled after the data breaches and data theft were reported. The voter registration database should be responsibly and independently audited in advance of the general election to attempt to detect any malicious manipulation of the database that may cause voter disenfranchisement or disruption during the election. Voters should be notified of the known security breaches and asked to verify their voter registration on line well in advance of the election dates.

In sum, if the remedial action described above is initiated immediately, the Secretary and the State Election Board have sufficient time and resources to ensure that Georgia citizens have a far more reliable and secure election system in the upcoming primaries and general elections, which will greatly enhance voter confidence. We look forward to your immediate response, and welcome any questions you may have.

Sincerely,

Bruce P. Brown

cc: Cary Ichter
Robert A. McGuire, III
William Brent Ney
Marilyn R. Marks
Laura Digges
William Digges, III
Ricardo Davis
Megan Missett
David D. Cross
Halsey G. Knapp, Jr.

EXHIBIT 2

OFFICIAL ELECTION BULLETIN

August 1, 2018

TO: **County Election Officials and County Registrars**

FROM: **Chris Harvey, Elections Division Director**

RE: **Response to Coalition for Good Governance Communication**

Dear County Commissioners and Officials,

I am writing to you as the State of Georgia's Elections Director, a position I have held since July 2015. From August 2007 until July 2015, I was the Chief Investigator and Deputy Inspector General for the Secretary of State's office, investigating, among other items, potential violations of state election law. For over a decade, it has been my job to be intimately familiar with both Georgia election law, systems, processes, and procedures.

Before joining the Secretary of State's office, I was the Director of the Cold Case Homicide Unit with the Fulton County District Attorney's office where I investigated previously unsolved homicides. Prior to that role, I was the Chief Investigator with the DeKalb County District Attorney's Office where I led investigations in all crimes, including public corruption. Over my career in law enforcement, it has been my intention to serve Georgia by promoting public safety, security and fidelity to the law.

Throughout my tenure at the Secretary of State's office, election security has been a top priority for me personally, as it is for the entire Secretary of State's office and county election officials. Now more than ever, and especially since the election of 2016, voting security is featuring more prominently as a topic of national conversation. However, it has been a way of life in the Secretary of State's office for far longer. I write to you today to explain some of the protections that we, along with county election officials, have in place to ensure that Georgia's elections are secure and ask for your assistance in continuing to ensure secure elections in our state.

Elections in Georgia are a partnership between the state and the counties. County election officials run elections while the Secretary of State's office maintains the voter registration database and provides support to the counties. We work with your county election officials every day, and these hard-working public servants are truly the linchpin of our democracy.

Long before the public spotlight turned to the realm of elections, we recognized the real threat of people and entities - both foreign and domestic – seeking to interfere with our electoral process.

To combat this threat, we work with federal, state, local, and private sector partners every day, and we are continually adding additional levels of both cyber and physical security to Georgia's election system. It is our duty to provide Georgians with the opportunity to vote on a secure and reliable voting system, which we regularly test to ensure ongoing compliance with state law and State Election Board rules.

Georgia's election system consists of many components, including the voter registration system, election management system, voting machines, and election night reporting website. Strict security mechanisms surround each component. These safeguards include, but are not limited to, frequent password changes, brute force and inactivity account disabling, and two-factor authentication. Many people are pleasantly surprised to hear that Georgia builds its encrypted ballot databases on machines which are never connected to the internet—a safeguard which many other states have not yet implemented. We also deploy cybersecurity protections, secure armed transport of election materials, and physical security for our voting machines. Your county election officials are familiar with these processes and treat them with the utmost importance.

Recently, some county boards have received communications from parties who filed a federal lawsuit against Georgia to stop the use of voting machines – Direct Recording Electronic (DRE) equipment – and demand hand-counted paper ballots. In these communications to you, they mistakenly cite a state law which was superseded by a newer law for the assertion that counties can unilaterally elect to stop using DRE voting equipment. Their assertion is not an accurate statement of Georgia law.

In 2003, Georgia moved to a state-wide, unified system in 2003. O.C.G.A. § 21-2-300 (a) states, "Provided that the General Assembly specifically appropriates funding to the Secretary of State to implement this subsection, the equipment used for casting and counting votes in county, state, and federal elections shall, by the July, 2004, primary election and afterwards, be the same in each county in this state and shall be provided to each county by the state, as determined by the Secretary of State." Further, O.C.G.A. § 21-2-381 requires absentee in-person ballots (early voting) to be on a DRE and O.C.G.A. § 21-2-379.7, which requires at least one DRE unit accessible to handicapped voters to be placed in each precinct, and State Election Board rules align with both of these statutes.

There are some who believe that because the current DRE machines are fully electronic, there is no way to verify that voter selections match the vote count's output. This belief is not true. There are numerous ways to ensure that our voting machines are accurately counting votes, and election officials test and demonstrate the accuracy of these machines through logic and accuracy testing before every single use. Last year, the state also conducted a re-examination of the voting machines to ensure accuracy. In each of the three selected counties, each machine's output exactly matched its input on simulated election day conditions. Furthermore, on election days in 2018, the Secretary of State's office conducts parallel testing, which means we take an actual county's ballot database and run a mock election to ensure that output matches the ballot selections. In each instance, the machine's output has exactly matched the selections. We have never taken accuracy for granted. It is constantly tested and re-tested.

There is a provision of Georgia law that allows the state to move to paper ballots in the event that the machines are "inoperable or unsafe." If we ever reach a point where our office feels that these

machines cannot be trusted to accurately deliver election results, we will invoke this statutory provision. To this day, there is no credible evidence that our election process is anything except secure and accurate.

While we are confident in the integrity of our elections, we remain vigilant and committed to ensuring that the confidence of Georgia voters in their elections and government is well-deserved. The Secretary of State's commitment to constant vigilance is why we have supported a move towards a new voting system to replace the current, aging system in a responsible fashion. This year, Secretary Kemp appointed the bi-partisan Secure, Accessible, and Fair Elections (SAFE) Commission, which consists of numerous county election officials, legislators, election law experts, a cybersecurity expert, and an accessibility expert. The SAFE Commission, working with our office, will present recommendations to the General Assembly by this January on how to responsibly move to a new system.

As county officials, we recognize the role that you play in keeping our system secure and accurate. The Secretary of State's Office values our county partners who work hand-in-hand with county elections boards and officials to run Georgia's elections. Thank you for your continued support and dedication to secure elections in Georgia. Please feel free to contact me directly with any questions.

Sincerely,

Chris Harvey

State Elections Director

DECLARATION OF JASMINE CLARK

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

DONNA CURLING, et al.	)	
	)	
Plaintiff,	)	
	)	**CIVIL ACTION FILE NO.:**
vs.	)	**1:17-cv-2989-AT**
	)	
BRIAN P. KEMP, et al.	)	
	)	
Defendant.	)	
	)	

DECLARATION OF JASMINE CLARK

JASMINE CLARK hereby declares as follows:

1. I am have been a Georgia voter since 2006 and am currently registered to vote at 280 Braxton Place in Gwinnett County. I have been continuously registered to vote at this address since 2016.
2. My precinct is Lucky Shoals Park and my polling place is located at 4651 Britt Rd, Norcross, GA.
3. I have not made changes to my voter registration while living at this addresss.

4. I am a candidate for Georgia House of Representatives District 108 in the upcoming November, 2018 election.
5. As a candidate, I have become aware of chronic problems in Georgia's electronic election system and I follow the news of Georgia voting problems. I followed news reports of the security failures and breach of the KSU election server and voter files, as well as numerous problems reported with incorrectly assigned districts such as the inaccurate voter assignments of approximately 600 voters reported in House District 81. [1]
6. I frequently visit the My Voter Page section of the Secretary of State's website (https://www.mvp.sos.ga.gov/MVP/mvp.do) as I campaign and help voters check their registrations, which I routinely encourage them to do.
7. I frequently verify my own registration to be certain that unauthorized changes have not been made. I am aware of the security breaches in the voter files and want to be certain that my registration is never affected.

---

1 https://politics.myajc.com/news/state--regional-govt--politics/doraville-voters-might-have-been-given-wrong-ballots/XIyZEXgkEwhuV4q9hrdFvM/

8. On Election Day, July 24, 2018, I arrived at my precinct polling place at 4651 Britt Rd, Norcross, GA at approximately 7:50 a.m., planning to vote before going to work.
9. A person in line in front of me at the voter check-in table was turned away without voting as I overhead the poll worker tell him that he was in the wrong polling place, although he insisted that it was his traditional polling place. I wondered if discrepancies were being encountered with the electronic pollbooks in my polling place.
10. I presented my drivers license and after the poll official checked the electronic pollbook, he told me that I was not in the pollbook for precinct 012 but that I must go to the Chinese Christian Church on Britt Rd., another precinct nearby, but in a different District.
11. I was completely confident of my polling place precinct assignment and location and refused to leave, but instead made phone calls and inquiries to try to vote in my polling place on a regular (not provisional) ballot.
12. I talked with the precinct workers and managers and was repeatedly told that I was in the wrong precinct polling location and not on the electronic voter list for precinct 012.

13. I opened my smart phone and pulled up my information on My Voter Page and showed the workers that I was present in the correct precinct according to the live Secretary of State's website. They contined to insist that the electronic pollbook showed my voting location at another precinct polling place, and would not issue a ballot for my precinct to me.

14. After spending approximately 25 minutes on the phone trying to resolve my problem, pollworkers told me that suddenly my name had appeared on the electronic pollbook for that voting location. There was no explanation offered as to how this was possible after so many election officials had previously checked the records, reportedly finding that I was not eligible to vote in this precinct 012.

15. I was issued a voter access card and voted my electronic ballot on the touchscreen machine without incident, although I had spent at least a half-hour more at the polls than I had planned. Unlike other people I met that day who were turned away, I had the flexibility to stay to fight for my right to vote in the right precinct on the correct ballot.

16. Although I had no logical explanation for what happened, I took the first opportunity at approximately 10 am that morning to record and post a video to Facebook[2] to explain my experience to other voters and offer advice on what to do if they encountered voting problems because of their pollbook or voter registration issues.

17. Both as a candidate and a citizen, I am deeply concerned about the security failures of the electronic voting system, and the discrepancies and errors in the electronic pollbooks that disenfranchise and discourage people from voting.

18. I heard people in the precinct 012 polling place who were turned away say that they did not have time to travel to another polling place. I did not hear pollworkes offer them a provisional ballot, making it likely that these people did not get the opportunity to vote.

19. I plan to vote in the November 2018 election and based on my experience, I am concerned that I may be given an inaccurate ballot, or that my name may not be found in the pollbook, or that I will be otherwise disenfranchised.

[2] https://www.facebook.com/annakellyleary/posts/10155422963347096

20. As a candidate, I am concerned about voters in my district potentially being disenfranchised and the impact on my House District 28 race and all other races on the ballot.

21. As additional voting problems are discovered and exposed, I expect that voters will be discouraged from voting and voter confidence will continue to diminish, along with voter turnout, if the immediate corrections are not made to the election system.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, July 31, 2018.

Jasmine Clark

DECLARATION OF KIMBERLY C. COPELAND

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

DONNA CURLING, et al.	)	
Plaintiff,	)	
vs.	)	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**
BRIAN P. KEMP, et al.	)	
Defendant.	)	

DECLARATION OF KIMBERLY C. COPELAND

KIMBERLY C. COPELAND hereby declares as follows:

1. I am a Georgia voter registered to vote at my residence at 3420 Meadow Lane, Gainesville, Georgia, 30506.
2. I served for 11 years on the Hall County Board of Elections until November 2017. I am currently the Chairman of the Hall County Democratic Committee. My role in the county Democratic Party includes promoting voter rights, election integrity, voter registration, supporting our candidates' campaigns and voter turnout.
3. On May 22, 2018, late in the evening of Primary Election Day, I received a call from Alana Watkins, Democratic Party candidate for House District 30. She reported that she had just visited her home Precinct 10 (Candler) polling place at Hopewell Baptist Church, 5086 Poplar Springs Rd, Gainesville,

Georgia, 30507, on her way home from our victory party to review the machine results tapes posted on the door. She reported that one tape did not contain her race. I told her that I would investigate.

4. I went to the Candler polling place that night a little before midnight. I observed ten DRE voting machine results tapes posted on the door. I observed one results tape that was missing the House District 30 race as Ms. Watkins had reported, and was also missing several other races such as the Congressional District 9 races, and County Commissioner races, among others.
5. At approximately 11:58 pm, I took the picture as Exhibit A of the portion of the results that was missing races. I also shot a short video of the results tape comparing it the other tapes posted on the door. It is posted at: https://www.dropbox.com/s/ea0599yeo5kiy5u/Candler%20election%20tape.mp4?dl=0.
6. I examined the tape and confirmed that there were no tears, folds or other signs of a change in the tape that could account for the missing data.
7. I provided copies of the photograph (Exhibit A) and video recording (Exhibit B) to Ms. Watkins, state party officials, and Dana Bowers of the Josh McCall campaign for the 9th Congressional District for follow up.

8. I have been involved in Hall County election mechanics and reporting for over 10 years. I had never before seen a machine tape posted that is missing races, so this naturally concerns me as to the extent to which such malfunctions can impact or alter the vote on the paperless unauditable machines.
9. In addition, on Primary Election Night, I noticed the election results from Hall County were unusually late in being reported. Michelle Jones of the Hall County Board of Elections reported she was told that about one-half of the voting machines in the county were experiencing problems closing down.
10. I have not received further information on the nature of the reported machine shutdown issues.
11. I am concerned about the inability to recount, verify, or audit Georgia's election results from the electronic voting system without a paper audit trail.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, August 2, 2018

Kimberly C. Copeland

EXHIBIT A

TIMES COUNTED 75
TIMES BLANK VOTED 15
C. EATON (I) 60
****
PSC Eaton- D
RACE # 91 PARTY:DEM
RUNNING 3
TO VOTE FOR 1

TIMES COUNTED 21
TIMES BLANK VOTED 4
L. MILLER 11
J. NOEL 3
J. C. WHITE 3
****
PSC Pridemore- R
RACE # 95 PARTY:REP
RUNNING 2
TO VOTE FOR 1

TIMES COUNTED 75
TIMES BLANK VOTED 11
J. HITCHINS III 30
T. PRIDEMORE (I) 34
****
PSC Pridemore- D
RACE # 96 PARTY:DEM
RUNNING 2
TO VOTE FOR 1

TIMES COUNTED 21
TIMES BLANK VOTED
RACE # 476 PARTY:REP
RUNNING 1
TO VOTE FOR 1

TIMES COUNTED 74
TIMES BLANK VOTED 9
B. THOMPSON (I) 65
****
BOE At Large - D
RACE # 477 PARTY:DEM
RUNNING 1
TO VOTE FOR 1

TIMES COUNTED 19
TIMES BLANK VOTED 4
S. LOPEZ 15
****
BOE 1 - R
RACE # 479 PARTY:REP
RUNNING 1

ECLARATION

DECLARATION OF ROB KADEL

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

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF ROB KADEL

I, ROBERT S. KADEL pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. I am a registered voter in DeKalb County, Georgia, and registered to vote at my home address of 2426 Sherbrooke Ct. NE, Atlanta, GA 30345.
2. I am employed by the Georgia Institute of Technology as Assistant Director for Research in Education Innovation, Center for 21st Century Universities.
3. As a Georgian, a sociologist (Ph.D., Emory University, 1998), and a research volunteer on Georgia's election processes, I have sought a greater understanding of the operation of touchscreen voting systems.

4. Therefore when I voted in advance voting on May 4, 2018 at The Gallery at South DeKalb Mall in Decatur, Georgia, I was attentive to the details of the voting process.
5. Prior to voting, I had accessed the Georgia Secretary of State's website to check my registration details and print a sample ballot for races and questions for which I am eligible to vote.
6. I carried my marked sample ballot with me to the polling place for reference.
7. I arrived at the polling place at approximately noon, and there were very few people in the polling place.
8. I filled out the paper form for application for early voting and handed a poll worker that completed form and my driver's license. The poll worker verified my information and signature and then asked me to take my license and the form to another table with four laptops on it.
9. At that table, I gave the poll worker my form and license. She scanned my license barcode and handed it back, then she gave me an activated yellow voter access card with which to initiate the voting process on the touchscreen machine.
10. I used a machine with serial number 116649.

11. I selected choices in the races for Governor and a few others and then noticed that the electronic ballot presented on the screen displayed Congressional District 5 and State Senate District 44.
12. I live in Congressional District 6 and State Senate District 42, and was alarmed to see races to vote for which I am ineligible, and to see that my electronic ballot was missing races for which I am eligible to vote.
13. I alerted a poll worker who alerted her supervisor, Ms. Atkinson, who was managing certain areas of the polling place that I had an incorrect ballot.
14. The poll worker whom I had alerted held her finger on the “page" button at the bottom of the machine screen for about 10 seconds and then cancelled my ballot and ejected the card.
15. The poll worker and I walked over to the table of laptops where they were coding the yellow voter access cards, and I explained that I should be voting in Georgia Congressional District 6 and Georgia State Senate District 42.
16. The poll worker said that if I was seeing “Georgia 5,” it is because I live in “Georgia 5.”
17. I told her that I had voted in the Georgia’s 6th Congressional District Special Election last year.

18. I have not changed my residence since voting in the 6th District Special Election in 2017.
19. The poll worker called over Ms. Atkinson who looked at the sample ballot I had brought with me (to indicate which candidates I wanted to vote for). The supervisor said that I had a nonpartisan ballot that wouldn't have shown any races.
20. I corrected her and said that this was the Democratic sample ballot that I had printed at home, and that she could see that it had the Stacey Abrams / Stacey Evans race for Governor at the top.
21. Ms. Atkinson instructed another poll worker to re-enter my information into a touch screen device sitting on the table (operated with an electronic stylus), and then they finally saw that I had been presented with the wrong ballot.
22. They generated a new yellow voter access card for me at that time, which was approximately 12:11 pm.
23. The original poll worker with whom I had spoken walked back with me to the machines and I voted on machine serial number 158583.
24. The poll worker watched me insert my card and asked if I would quickly hit the Next button to get to the screens with the congressional races and

verify that I was presented with the correct races on the electronic ballot. I did that, and all looked correct.

25. The poll worker then left to provide voter privacy, and I skipped back to the beginning and began making my electoral selections.

26. I cast that electronic ballot on the touchscreen machine at 12:15 p.m.

27. I walked to another table and returned my yellow card to another poll worker. She asked me if I had time to take a survey, and I said that I really needed to get going.

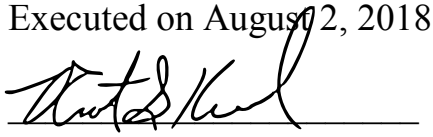
28. Based on my personal research and my May 4, 2018 voting experience, I do not believe that the DRE voting system can be relied on to produce accurate election results. However, I still desire to vote in the November 2018 election.

29. I plan to vote by mail-in paper ballot to ensure that I can thoroughly check the accuracy of the ballot issued to me and that my vote can be verified and recounted if necessary. If I vote by mail, I will incur additional inconvenience of requesting and voting a mail ballot in order to case a more secure ballot. I would prefer to maintain the flexibility to vote in my neighborhood precinct on Election Day when all last-minute campaign information is available. However, if paper ballots are not available at the polling place, I will be forced to choose between casting

a verifiable paper ballot and giving up my ability to vote on Election Day in my local polling place.

I DECLARE UNDER PENALTY OF PERJURY THAT THE FOREGOING IS TRUE AND CORRECT.

Executed on August 2, 2018



Robert S. Kadel

DECLARATION OF LOGAN LAMB

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

DONNA CURLING, ET AL., **Plaintiffs** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF LOGAN LAMB

LOGAN LAMB hereby declares as follows:

1. I am a cybersecurity researcher based in Atlanta, Georgia.

2. I have a Bachelor of Science degree and a Master of Science in computer engineering from University of Tennessee, Knoxville.

3. I have worked professionally in cybersecurity since 2010 where I started at Oak Ridge National Lab in the Cyber and Information Security Research group. In that position, I specialized in static and symbolic analysis of binaries, red-teaming prototype critical infrastructure, and de-identifying geospatial data.

4. I left that operation in 2014 and joined Bastille Networks, a local cyber-security startup business where I am still employed. At Bastille Networks I specialize in wireless security and applications of software defined radio.

DREs are not and will never be secure

5. A DRE (direct-recording electronic) is a voting machine which records votes electronically. DREs do not have a voter-verified paper audit trail, meaning there

is no way of auditing the results of an election. A voter-verified paper audit trail allows voters to independently verify that their vote is being recorded as intended, which is impossible with DREs since the sole record is an electronic copy, and the voter cannot determine how his vote was recorded. Since the only copy of the electronic vote is stored on the machine, there is no way to independently verify the votes cast by voters. If an ostensible audit were to be conducted on DREs, at best this audit would verify the DREs are functioning in a deterministic manner (benign or malicious) at the moment it is being tested. At worst, if the audit results differ from the original then the machines are not functioning in a deterministic manner and the results of the election cannot be trusted, and, unlike paper ballot elections, such errors cannot be remedied.

6. This inherent design flaw, the lack of a voter verified paper trail, means if there are any flaws in how the paperless DRE records votes, then there is no way to detect or correct any mistakes during a post-election audit.

My experience with Diebold voting machines

7. In my research with Diebold AccuVote TS and TSx machines, (the DRE models used in Georgia) I rely on a wealth of academic research conducted detailing how Diebold voting machines have never been a secure way of recording votes, and have known vulnerabilities which call into question results.

8. Motivated by Kohno et al., TTRB, and EVEREST, (see Bernhard Declaration, *passim*) I have begun writing software to independently verify a selection of vulnerabilities of the Diebold AccuVote voting system detailed in those studies. My focus has been on developing methods to quickly verify that the version of software currently used in Georgia, Ballot Station 4.5.2!, is vulnerable to known attacks identified in the academic research. If 4.5.2! is found to be vulnerable to these select attacks, then

it is highly likely that Georgia's version of software is also vulnerable to other attacks detailed in the academic research.

9. Even without running this software to verify likely vulnerabilities affecting version 4.5.2!, the software should be assumed to have critical vulnerabilities since other version of software including 4.3, 4.6, and 4.7 (released before and after 4.5.2!) have had critical vulnerabilities affecting them.

10. I have written software to decrypt ballot results files for BallotStation 4.3.15 and see how votes were cast in order, violating voters' secret ballot protections. I have also created smart-cards which can record the *Smart Card Key* as detailed in EVEREST report (13.3.7). This is the first step in creating illegitimate supervisor cards and infinite voter cards, permitting an unlimited number of votes to be cast by the voter. This vulnerability almost certainly affects 4.5.2! since it affects versions created before and after the Georgia version. I've also written software which is capable of decrypting the file *bs-security.cf* (EVEREST 13.3.5). EVEREST says this attack, "creates the potential for more serious attacks. For instance, malicious software (i.e., a virus) could use this knowledge to alter election results, erase system logs and/or leak the keys necessary to create fraudulent smart cards (e.g., Voter Cards)."

KSU server findings and implications

11. On August 23, 2016 I went to the Fulton County Elections Department 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 conduct a wireless security assessment as a research project. There I was told to contact Merle King at Kennesaw State University because all election equipment was at that time managed by the Center for Election Systems at KSU.

12. On August 24, 2016 I intended to contact Merle King. Prior to doing so, I wanted to check the CES public website to see if there were any public documents that could give me background on CES and Merle King's duties. 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.

13. When a search engine like Google caches a file, the search engine makes a local copy of the file in case the original link to the file becomes unavailable. Google had already made copies of some of these files on the CES server prior to my accessing them. So, even if CES were to rectify the situation and remove the files from its web server, Google would still have a copy, generally making it available to the public without authorization

14. After this discovery, I wrote a quick script (simple program) to download what public files were available from the CES server here: https://elections.kennesaw.edu/sites/ , at the time a publicly accessible site. No passwords or authentication were required to gain access to these sensitive files. 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:

a. voter registration databases filled with personally identifiable information of over six million voters (filename *PollData.db3*). The data included driver's license numbers, birthdates, full home addresses, the last four digits of social security numbers, and more.

b. Election Management System GEMs databases (.gbf and .mdb extensions) GEMS is the central tabulator of the voting system, and used to create ballot definitions, program memory cards and tally and store and report all votes when

an election closes. I was able to access and download GEMS databases for at least 15 counties. These GEMS databases use poor encryption, allowing third parties to extract usernames and passwords for multiple databases.

c. Multiple training videos, of particular interest *CES-BulkUpdate_Final.mp4*. This video details how to update the voters' list containing private and personal voter information using a file downloaded over the internet from elections.kennesaw.edu. The video details navigating to elections.kennesaw.edu, logging into the website, downloading *PollDataUpdates.db3*, placing this file on a memory card, inserting that card into an ExpressPoll Unit (the electronic pollbook), and finally applying the absentee update to the ExpressPoll unit. It appears the counties Fulton, Cobb, Dekalb, Gwinnett, Forsyth, Chatham, Muscogee, Henry, Columbia, Clayton, and Cherokee download files from elections.kennesaw.edu and put those files on ExpressPoll units for use in the polling places to validate voters and issue electronic ballots. (I have attached as Exhibits 1 and 2 are collections of documents that I understand were produced by KSU in 2017 in response to an Open Records Act Request. The records referred to in this paragraph appear on Exhibit 1, page 27).

d. PDFs of election day supervisor passwords, for example, *July 2016 Primary and NP Election Runoff Password Memo.pdf*. Supervisor passwords control the administration of the DRE voting machines in the polling place including opening and closing of the voting machines as well as making administrative corrections when machine problems are encountered.

e. Windows executables and DLLs, for example:

- *System.Data.SQLite.DLL*
- *ExpDbCreate.exe*
- *ExpReport.exe*

15. It appears these files are used by the Diebold ExpressPoll (electronic pollbook) units. Since ExpressPoll units are specialized Windows PCs, an attacker can modify theses files and affect the behavior of the ExpressPoll units at the polling place when voters are checked in to vote, assigned a particular ballot style, and approved for voting. A list of vulnerabilities affecting ExpressPoll units is located on the internet at the following URL: https://github.com/josephlhall/dc25-votingvillage-report/blob/master/notes-from-folks-redact.md

16. On August 28, 2016 and August 29, 2016, I contacted King by email and telephone to warn him that CES should assume that the sensitive documents hosted on the "elections.kennesaw.edu" server had already been downloaded by unauthorized persons. Yet for reasons that have never been explained, the server was not secured for months. Along with my colleague Christopher Grayson, I accessed the server again several times in late February 2017 and was able to access and download the same types of files that I had accessed months earlier.

17. Besides making the above information available to the public, the server at elections.kennesaw.edu ("Election Server") was running a version of Drupal, a widely-used content-management framework for websites, which is vulnerable to an exploit called "drupageddon." Using drupageddon, an attacker can compromise a vulnerable server with ease. A public advisory for drupageddon was released in 2014, alerting users that an attack, "can lead to privilege escalation, arbitrary PHP execution, or other

attacks." In practice this means an attacker could have created, modified, or deleted files on the web server, likely without detection.

18. Drupal assigned this vulnerability the highest security risk score possible, 25/25 (Highly Critical).

19. Drupal released a tool to help with the identification of vulnerable servers, called Drupalgeddon (with an L), and made the following critical warning regarding the use of the tool:

> "Drupalgeddon drush command is only useful when restoring from backups is not an option and sufficient expertise is available to attempt a labourious manual recovery. Even then, **neither Drupalgeddon nor an expert can guarantee a website has** not **been compromised.** They can only confirm with certainty that a site *has* been compromised. This is because:
>
> - Drupageddon attacks may not leave any trace at all
> - Attacks that do leave traces change faster than what Drupalgeddon maintainers can keep up with
> - It is impossible to think of all the places that attackers might hide a backdoor.
> - **There are known exploits that Drupalgeddon does not yet check for.** Contributions are welcome (see below).
>
> If you decide to use Drupalgeddon; **Good luck to you; You will need it.**"

20. Based on internal CES staff emails obtained in public records, management was fully aware of the severity of these vulnerabilities, noting that elections.kennesaw.edu was identified as having "a number of critical and severe vulnerabilities some of which are reported to be exploitable" in September 2016 and "40+ critical vulnerabilities" in October 2016. (The documents referred to in this paragraph may be found on pages 40 and 34 of Exhibit 2.) The fact that the server was allowed to remain online for months until notified again of vulnerabilities is completely inexcusable in my opinion.

21. It is my opinion that the Diebold DRE-based election system and its components should not be used in a public election. It is my opinion that the system, given the level of exposure it was and is still presented with, must be assumed compromised, which necessitates a thorough scrubbing of every component and reinstallation of vendor's certified software. Even after a thorough scrubbing of every component, without software updates to remedy vulnerabilities the risk of compromise and implantation of malware still remains high.

22. From the training video *CES-BulkUpdate_Final.mp4* and open records, we know files from the internet-accessible website elections.kennesaw.edu, a vulnerable server, are placed on ExpressPoll units. This means an attacker could have had a straightforward attack-chain of remotely compromising elections.kennesaw.edu and implanting malware on files that are placed on ExpressPoll units, directly compromising the purportedly "air-gapped" system. Although this particular server no longer operates in the state's election administrative operation, any malware that may have been introduced during periods of security failure would very likely still be present on ExpressPoll books or on the other voting system components which remain in use across the state.

23. The system is flawed by design and made worse by the KSU exposure in ways that cannot be practically mitigated. The system should be treated as untrustworthy for the conduct of Georgia's elections.

Poor Physical Security Affecting Voting Systems

24. I have visited the Fulton County Election Preparation Center on multiple occasions, and have been able to freely roam the facility at times. While observing public

logic and accuracy pre-election testing of voting machines with colleagues, on one such visit I noted:

a. A stack of unsecured supervisor cards, which operate the DRE voting machines;

b. Multiple unsecured voter access cards, which are used by voters to activate their electronic ballot on the DRE;

c. A box of unsecured DRE memory cards;

d. A paper printout of a supervisor password;

e. Multiple unsecured Accuvote TS machines with the hinged door which protects the memory card slot unlocked. (These machines were also powered on. An attacker could have easily inserted a malicious smart card or memory card into these machines.); and

f. The cameras on the interior of the building do not have full view of the facility, an attacker can easily gain access to machines while out of view of the cameras.

An attacker could have easily stolen or modified the various unsecured pieces of election hardware.

25. On July 24th, 2018 my colleagues and I observed the closing of the polls at Grady High School. After the polls were closed, my colleagues and I were left unattended for the evening with the voting machines in the school gymnasium. The only measures taken to secure these voting machines were:

a. A cable lock binding all the voting machines together;

b. Tamper evident seals on the machines; and

c. A single security camera.

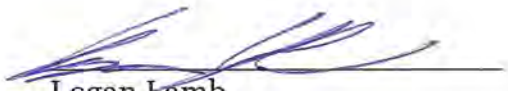
26. An attacker could have easily disabled the security camera and then modified or stolen the voting machines. The machines were secured with tamper evident seals which can be purchased on the internet at the following URL: http://www.intab.net/Large-Pull-Tite-Seals/productinfo/03-1330/003%20BLUE/

Summary

27. Based on my personal observations, research and knowledge of the authoritative academic studies, it is my opinion that the use of the Diebold DRE voting machines should be immediately curtailed, and not permitted for use in Georgia's elections. Remaining components of the Diebold DRE-based voting system such as the GEMS server, AccuVote optical scanners, and the ExpressVote electronic pollbooks must undergo decontamination procedures prior to use in future elections.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, August 3, 2018.



Logan Lamb

EXHIBIT 1

Michael Barnes

From: Steven Dean <stevendean@kennesaw.edu>
Sent: Wednesday, March 15, 2017 10:51 AM
To: Michael L. Barnes; Merle Steven King
Subject: Request for data retrieval from elections.kennesaw.edu

We would like to retrieve certain records from elections.kennesaw.edu, including equipment inventory records and workflow databases used during ballot building. These data are located in the *cesuser* user directory at /home/cesuser. We would like to retrieve the entire *cesuser* directory.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

From: Stephen Craig Gay
To: Lectra Lawhorne
Subject: CES Investigative update
Date: Friday, March 17, 2017 5:11:58 PM

Lectra,

Good afternoon. I wanted to take a moment and provide you with an update on the Center for Election Systems Incident Response process:

- We met with CES Staff today to review the architecture of their internal network, review physical access controls, and understand the services running on the internal network. We validated that an air gap exists between the internal and external network and further validated via arp tables that no routes were available from the intranet servers to an external network. Several opportunities for improvement were identified and CES staff are working on documentation for the system. An executive summary with recommendations is forthcoming

- All external-facing servers associated with the Center are isolated to elections.kennesaw.edu which is hosted in the Enterprise instance of OmniUpdate and contains only public information.

- UITS WinServ, in partnership with the ISO and CES, is provisioning a dedicated Virtual Server which will be used for internal file storage for CES. The server will be locked down via AD group memberships and will use verbose logging and monitoring tied to our splunk instance. The logs will specifically audit for file access and alert on any modifications to the authorizing AD group. Furthermore a local firewall will be in place and all traffic outside the CES IP range blocked.

- I met with FBI Agent Ware at 4:30pm to receive the elections server - Dell PowerEdge R610 Tag Number 96J2F21. The ISO team will be performing a data recovery for data requested by the CES (Business Operations) on Monday. We have confirmed that the FBI is maintaining a forensic image and changes to the server can occur. Agent Ware shared that "the investigation is wrapping up" and mentioned being in attendance at the March 29th meeting with AUSA Grimberg.

Please let me know if you have any questions or if I can provide any additional information.

In service,

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

Milestone	Due Date	Status	Lead	Notes
Private Network Assessment Meeting	26-Jun	Complete	S. Gay	
Spec UPS	13-Jul	Complete	C. Dehner	
Order UPS	13-Jul	Complete	C. Dehner	
DBAN R610 Hard Drives	7-Jul	Complete	C. Dehner	
Deliver R610 to Networking	7-Jul	Complete	C. Dehner	
Image Dell PowerEdge R630s (101614 & 101613)	26-Jul	Complete	C. Darrow	
Rack Dell PowerEdge R630 and migrate DC and NAS	28-Jul	In progress	C. Darrow	
Install UPS	4-Aug	Complete	C. Darrow	Due data dependant on delivery of UPS from CDW-G.

192.168.3.135	Linux 2.6.8	•M6600M85		IMI Card Duplicator	
192.168.3.119	Linux 2.6.8	•M6600M73		IMI Card Duplicator	
192.168.3.81	Linux 2.6.8	•M6600M80		IMI Card Duplicator	
192.168.3.73	Linux 2.6.8	•M6600M72		IMI Card Duplicator	
192.168.3.116	Linux 2.6.8	•M6600M82		IMI Card Duplicator	
192.168.3.104	Linux 2.6.8	•M6600M70		IMI Card Duplicator	
192.168.3.115	Linux 2.6.8	•M6600M71		IMI Card Duplicator	
192.168.3.130	Linux 2.6.12	•M6600M81		IMI Card Duplicator	
192.168.3.76	Linux 2.6.8	•M6600M69		IMI Card Duplicator	
192.168.3.123	Linux 2.6.8	•M6600M26		IMI Card Duplicator	
192.168.3.128	Linux 2.6.8	•M6600M79		IMI Card Duplicator	
192.168.3.131	Linux 2.6.8	•M6600M84		IMI Card Duplicator	
192.168.3.71	Linux 2.6.8	•M6600M83		IMI Card Duplicator	
192.168.3.132	Linux 2.6.8	•M6600M86		IMI Card Duplicator	
192.168.3.69	Linux 2.6.8	•M6600M417		IMI Card Duplicator	
192.168.3.66	Linux 2.6.8	•M6600M74		IMI Card Duplicator	
192.168.3.2	Microsoft Windows Server 2003 R2 SP2	•SEMINOLE			
192.168.3.53	HP P2055 Series	•Fax-Printer •FAX-PRINTER			
192.168.3.55	Microsoft Windows XP	•SDEAN-GEMS-2			
192.168.3.57	Microsoft Windows XP	•CALLCENTER			
192.168.3.50	Microsoft Windows Server 2008 R2, Standard Edition	•EPIC			
192.168.3.4	Microsoft Windows Server 2008 R2, Enterprise Edition	•CES-DC1			
192.168.3.3	Microsoft Windows Server 2008 R2, Standard Edition	•CES-NAS			
192.168.3.1	Microsoft Windows Server 2008	•CES-DC.CES.KENNESAW.EDU			
192.168.3.54	Microsoft Windows XP	•MPEARSO9-980			
192.168.3.56	Microsoft Windows XP	•GEMS-DDESSERT			
192.168.3.60	Microsoft Windows 7 Home, Premium Edition SP1	•STEVEN7-GEMS		Audio recording	
192.168.3.70	Windows XP	h57-marie.CES.KENNESAW.EDU			
192.168.3.65	Windows XP	GEMS-mking.CES.KENNESAW.EDU			
192.168.3.51	Microsoft Windows 7.5	•KSLICES-2HALL		Audio recording	
192.168.3.61	Unknown				
192.168.3.52	Windows XP	seminole-termin.CES.KENNESAW.EDU			

From: Christopher Dehner
To: Steven Dean; Jason Figueroa
Cc: Michael Barnes; Stephen Gay
Subject: CES server surplus
Date: Wednesday, August 9, 2017 11:24:58 AM

Fellas,

I will arrive at the center around 1:30 today to pick up the old DC. I will also get the old unicoi server from secure storage. Additionally, I sent in a service ticket for this request.

Regards,

Chris

Get Outlook for Android

STATE OF GEORGIA

FULTON COUNTY

AGREEMENT BETWEEN THE SECRETARY OF STATE

AND

THE BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA

This AGREEMENT ("Agreement"), made this 6th day of June, 2016, by and between the OFFICE OF THE SECRETARY OF STATE OF THE STATE OF GEORGIA (hereinafter the "Secretary of State") and the BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA through KENNESAW STATE UNIVERSITY, a unit of the University System of Georgia, (hereinafter "University") for the consulting services of the Center for Election Systems of KENNESAW STATE UNIVERSITY (hereinafter "KSU").

WITNESSETH

WHEREAS, the Secretary of State desires to employ the services of KSU to assist the staff of the Elections Division of the Office of the Secretary of State (hereinafter "the Elections Division") with: technical support and training of State election officials in the use of the Statewide uniform electronic voting system (hereinafter "the voting system") in the State of Georgia; acceptance testing for the fiscal year 2017 of the GEMS software, the direct recording electronic voting devices (hereinafter "DREs"), and the electronic poll book/encoders "ExpressPoll" which constitute components of the voting system; ballot building and related activities for counties and municipalities in the State of Georgia ("State");

WHEREAS, the Secretary of State has the authority under the Laws of the State of Georgia to enter into this Agreement; and

WHEREAS, the University is both qualified to enter into this Agreement and has offered such services to the Secretary of State under the terms and conditions stated herein; and

WHEREAS, the parties wish to enter into this Agreement under the terms and conditions set forth herein;

NOW THEREFORE, in consideration of the mutual promises and agreements hereinafter set forth, the satisfactory consideration each for the other hereby expressly recognized and agreed, the parties hereby contract for services in accordance with the following provisions.

ARTICLE I. SCOPE OF SERVICES

KSU will assist the staff of the Elections Division under the direction of and as directed by the Director of the Elections Division or his/her designee, in the following areas:

A. KSU shall maintain a "Center for Election Systems" (hereinafter "the Center") that will primarily provide technical and training support on the statewide uniform system to the Elections Division, Georgia election officials, county election board members and election superintendents;

B. KSU shall test the voting system for compliance with the Georgia Elections Code, as required under Article 9 of Chapter 21 of the Official Code of Georgia and under the Rules of the State Election Board and the Rules of the Secretary of State, as these laws and rules presently exist and may hereafter be amended. This testing to be conducted during Fiscal Year 2017 shall include, but is not limited to, the physical examination of software and voting equipment acquired by the Secretary of State or any County in the State of Georgia in connection with deployment of the voting system, and the preparation and submission of reports of such evaluations to the staff of the Elections Division;

C. KSU shall work with the vendor and the Elections Division to define the next versions of all components of the voting system;

D. KSU shall implement classes and training modules, using electronic media where possible, for the instruction of Election Superintendents and Voter Registrars in the use of the voting system;

E. KSU shall provide ballot building support for county election officials. KSU will provide office space and appropriate technical support for these services. KSU will coordinate the printing of paper absentee ballots;

F. KSU shall support the deployment of the ExpressPoll electronic pollbook, including preparation of compact flash memory cards with voter lists for each election and extraction of credit-for-voting data, post-election;

G. KSU shall support all State certification testing of voting systems and will provide acceptance testing for the State's voting system

H. KSU shall provide technical support for the State's election servers installed in the county election offices throughout the State;

I. KSU shall provide consultation and advice to local governments on the purchase, testing, and utilization of the software, voting equipment and other components which comprise the voting system;

J. KSU shall maintain a website that will provide an initial point of contact for election officials wishing to utilize the services of the Center. The website shall describe the various services available through the Center, provide directions for obtaining these services from the Center, and facilitate answers to "frequently asked questions";

K. KSU shall maintain a Help Desk designed for immediate response to problems encountered with any component of the voting system during the conduct of an election in any precinct. The Help Desk shall be staffed from 8:00 a.m. to 5:00 p.m. on all business days throughout the year, and from 6:00 a.m. until County tabulations are concluded on election days;

L. Upon request of the Secretary of State, KSU shall assist the Secretary of State with identifying, inspecting, and/ or implementing a new state wide voter registration system which will allow integration with the voting system;

M. Upon request of the Secretary of State, KSU shall provide key faculty/employees identified as the Executive Director, Director, and Assistant Director of KSU with Blackberry technology or equivalent email and messaging capabilities;

N. KSU shall coordinate the proper disposal of decommissioned voting system components at the direction of the Elections Division;

O. KSU shall provide consulting services to Secretary of State on legislation or pending legislation and laws affecting elections;

P. KSU shall provide any other election services as may be required by the Elections Division;

ARTICLE II. RESPONSIBILITIES OF KSU

KSU shall continue to maintain a permanent location on the KSU campus for the operation of the Center. The Center shall be operated and maintained by a full-time staff, including but not limited to, an Executive Director, a Center Director, a Center Assistant Director, technical support staff, and student assistants. The Center shall contain voting equipment and software, provided by the Secretary of State, necessary to completely define, setup and conduct a sample election. The Center shall maintain a ballot building facility to house Center staff and Elections Division staff for the purpose of building ballots for counties and municipalities.

KSU shall not possess, obtain, or acquire, either directly or indirectly, a pecuniary interest in any business entity involved in the development, manufacture, marketing, or sale of computer voting equipment or software during the term of this Agreement and for one year after the ending date of this Agreement.

Any software, databases, or other analytic tools obtained or developed in support of activities covered under this Agreement and any work product resulting from activities covered under this Agreement are the property of the Secretary of State and may not be offered or utilized by any other entity in any manner whatsoever, in whole or in part, without the written permission of the Secretary of State or a designee of the Secretary of State.

KSU shall deploy newly purchased property acquired by the Elections Division, only after consultation with the individual within the Elections Division designated by the Elections Division Director for such purpose.

KSU shall require all employees of the Center who have access to the system and system security measures to sign confidentiality agreements, as provided by the Secretary of State.

ARTICLE III. TIME OF PERFORMANCE

6 cert/cert 7 cert/cert

The period of this Agreement shall be from July 1, 2015, through June 30, 2016. Either party may cancel this Agreement upon thirty days written notice to the other party.

ARTICLE IV. COMPENSATION AND PAYMENT

For the satisfactory performance of its duties and obligations set forth herein, KSU shall be compensated for its services for the full year of this Agreement in the amount not to exceed $792,385.00, for the State fiscal year 2017, billable in 12 installments of $66,032.08. Invoices shall be submitted to the Secretary of State on a monthly basis. KSU's services shall include support for such professional services, including secretarial, student assistants, mail and express mail delivery, telephone, computer charges, computer equipment and software, photocopying and other staff expenses as set forth in Appendix "A" attached hereto and incorporated herein by reference KSU's services and obligations under this Agreement shall be completed at or prior to the time of final payment. In the event of cancellation under Article III, no further payments shall be required under this Agreement beyond the end of the month in which the cancellation is executed.

ARTICLE V. RETENTION OF RECORDS

KSU shall keep and maintain as records of the Secretary of State all records and other documents pertaining to the performance of this Agreement until the final payment of funds to

KSU by the Secretary of State pursuant to this Agreement has been completed. At such time, physical custody of the records and documents shall be returned to the Secretary of State.

The University and KSU shall give immediate notice by telephone to the Elections Division Director of the Secretary of State of any open records request made pursuant to O.C.G.A. § 50-18-70 *et seq.*, request for production of documents and things, or subpoena associated with any litigation relating to any computer programs, computer software, equipment, or any other documents, issues or materials relating to the Voting System or any of its components. The University and KSU acknowledge that computer programs and computer software may be exempted from disclosure when meeting the definitions and provisions of O.C.G.A. § 50-18-72(f) and that an open records request may affect State or vendor rights. The University and KSU shall deliver to the Elections Division Director a copy of any written open records request received by the University or KSU promptly by electronic transmission, facsimile or in any event within 24-hours of its receipt of the request. In so far as possible, the University and KSU will allow the Secretary of State prior opportunity to comment on any response to any open records request within this paragraph; however, such review shall be for the convenience of the Secretary of State, without responsibility or liability to the University or KSU.

ARTICLE VI. REPORTING AND AUDITING REQUIREMENTS

KSU shall provide monthly reports to Secretary of State to report the status of the Center's performance under the Agreement and the Center's progress toward fulfilling the requirements of the Agreement. KSU shall, if it has expended $100,000 or more during its fiscal year in State funds, provide for and cause to be made annually an audit of the financial affairs and transactions of all the Center's funds and activities. The audit shall be performed in accordance with generally accepted auditing standards. KSU shall, if it has expended less than $100,000 in a fiscal year in state funds, forward to the State auditor and each contracting State organization a copy of the Center's financial statements. If annual financial statements are reported upon by a public accountant, the accountant's report must accompany them. If not, the annual financial statements must be accompanied by the statement of the president or person responsible for the nonprofit organization's financial statements.

ARTICLE VII. MISCELLANEOUS

The University, KSU, and the Secretary of State further mutually agree as follows:

A. This Agreement constitutes the entire agreement between the parties and any amendments to this Agreement must be in writing.

B. The provisions of O.C.G.A. § 45-10-20, *et seq.* will not be violated by the parties to this agreement.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement, this 6th day of June, 2016

ON BEHALF OF THE SECRETARY OF STATE OF THE STATE OF GEORGIA:

Signature

Timothy K. Fleming
Print Name Title

Deputy SOS

Date: 5/15/16

ON BEHALF OF THE BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA AND KENNESAW STATE UNIVERSITY:

Carolyn Elliott Farris for Charles J Amlaner
Signature

Charles J Amlaner Vice President for Research
Print Name Title

Date: 6/6/16

Appendix A

Budget, FY 2017
Center for Election Systems, Kennesaw State University

Category	FY 2017 Proposed Budget	
Personnel		
Center Executive Director	$	70,800.00
Director	$	87,800.00
Assistant Director	$	56,500.00
Election Professional II	$	48,500.00
Election Professional II	$	44,900.00
Election Professional II	$	43,300.00
IT Sys Supp Pro II	$	41,200.00
IT Sys Supp Pro I	$	36,500.00
Salaries	$	429,500.00
Fringes	$	128,850.00
Salaries and Fringes	$	558,350.00
Student Assistants	$	33,000.00
Temporary Staff Assistants	$	10,000.00
TOTAL PERSONNEL	**$**	**601,350.00**
OFFICE/LAB SPACE RENT	**$**	**41,000.00**
TRAVEL	**$**	**20,000.00**

TELECOMM	**$**	**12,000.00**
SUPPLIES	**$**	**12,000.00**
COPYING	**$**	**2,000.00**
FREIGHT & SHIPPING	**$**	**20,000.00**
COMPUTERS/SOFTWARE	**$**	**12,000.00**
Indirects (10%)	**$**	**72,035.00**
TOTAL BUDGET	**$**	**792,385.00**

FD-597 (Rev 8-11-94)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

On (date) 3/17/17

item(s) listed below were:
- ☐ Received From
- ☑ Returned To
- ☐ Released To
- ☐ Seized

(Name) [illegible]

(Street Address) [illegible]

(City) [illegible]

Description of Item(s): [illegible]

Received By: [signature] (Signature)

Received From: William D. Mason II (Signature)

LAMB DECLARATION

FD-597 (Rev 8-11-94) Page 1 of 1

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

On (date) 3/3/17

item(s) listed below were:
- ☑ Received From
- ☐ Returned To
- ☐ Released To
- ☐ Seized

(Name) [illegible]

(Street Address) [illegible]

(City) [illegible]

Description of Item(s): [illegible]

Received By: _____ (Signature) **Received From:** _____ (Signature)

LAMB DECLARATION

Evidence Tag

Date	Tag No	Case No:	Location
March 2, 2017		20170302CES	Center for Elections Systems

Public Safety Officer(s) involved ___NA___

Description of Property

Server with DNS name elections.kennesaw.edu with KSU asset tag 103019

Signature of Witness	Signature of Person Received Property

Chain of Custody Receipt

Released by (Print and Sign)	Date	Purpose	Received by (Print and Sign)	Date
Merle King	March 2, 2017	Retrieving server after reported data breach. Server will be retrieved by the FBI by UITS ISO	Stephen Rose	1907 March 2, 2017
William Ware	3/3/2017	←Swap Released & Received by →	Stephen Rose	March 3 2017

From: Mariel Louise Fox
To: Stephen Craig Gay
Cc: Tamara Elena Livingston
Subject: Fwd: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus
Date: Wednesday, March 15, 2017 4:22:40 PM

Stephen,

Below is the communication thread among Steven Dean, Jeff Milsteen and myself.

I'll await your direction and guidance as to next steps in providing consultation to Steven regarding KSU records, and I will communicate that message to Steven shortly.

Thanks!

Mariel Fox
Director, Records & Information Management
Museums, Archives & Rare Books (MARB)
LB 216 MD 1704
Direct: 470-578-2225
Main: 470-578-6289

----- Forwarded Message -----
From: "Jeff Milsteen" <jmilstee@kennesaw.edu>
To: "Steven Dean" <sdean29@kennesaw.edu>
Cc: "Mariel Fox" <mfox32@kennesaw.edu>
Sent: Friday, March 10, 2017 1:38:30 PM
Subject: Re: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Steven,

Mariel forwarded your inquiry to me. I believe there are a number of issues here that will require some additional work. For example, some of the data maintained by the Center is, by contract, property of the Secretary of State. That data would be subject to the Secretary of State's records retention policies and presumably those records should either be returned to the SOS Office or, if appropriate, destroyed at their direction and pursuant to their policies. All other records of the Center would be subject to the retention policies of KSU and Mariel can probably help you with existing retention guidelines. The trick, of course, is to correctly identify and categorize those records.

I was not clear what was being asked with respect to FOIA requests. If the Center receives any open records requests, those should immediately be forwarded to the Legal Division for review. The requests themselves, like all other official records of the university, are subjection to our retention guidelines.

I hope this helps. If you have additional questions, please let me know. Thanks.

Jeff Milsteen
Chief Legal Affairs Officer

----- Original Message -----
From: "Mariel Fox" <mfox32@kennesaw.edu>
To: "Jeff Milsteen" <jmilstee@kennesaw.edu>
Sent: Friday, March 10, 2017 9:26:22 AM
Subject: Fwd: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Jeff,

This request (see below) for advice came from Steven Dean (sdean29@kennesaw.edu), IT Systems Support at the Center for Election Systems.

I spoke to him on the phone concerning what types of records to keep and how long to keep them, directing him to the State of Georgia retention schedules on the Georgia Archives website.

As to his question about FOIA requests, I said that for KSU open records requests, those are handled by Legal Affairs. But for the Center's records, I did not know. I told him I would forward this question to you.

Please let me know if you have any questions, of if you have any suggestions on how to handle such inquiries in the future.

Thank you!

Mariel Fox
Director, Records & Information Management
Museums, Archives & Rare Books (MARB)
LB 216 MD 1704
Direct: 470-578-2225
Main: 470-578-6289

----- Forwarded Message -----
From: stevendean@kennesaw.edu
To: "records2go" <records2go@kennesaw.edu>
Sent: Thursday, March 9, 2017 1:58:52 PM
Subject: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Date Available for Consultation: No in-person consolation needed.

REQUESTED BY: Steven Dean Phone# 470-578-2120

Campus: Kennesaw
Department: Center for Election Systems
Office Location: House 3205

Advice requested for:
Myself and my supervisor or manager.

Need advice on:
['Which records do we need to keep?', 'How long do we need to keep records?', 'Do we need to keep both hard copy and digitial files?', 'What are our records responsibilities?', 'Topic not listed above. Describe in comments.']

Additional comments:
In writing new policies for data storage for the Center, I'd like to see your written policies for data storage periods as relating to FOIA requests.

Preferred communication method: Email.

From: Mariel Louise Fox
To: Steven Jay Dean
Cc: Stephen Craig Gay
Subject: Fwd: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus
Date: Wednesday, March 15, 2017 4:27:49 PM

Steven,

I just learned that Stephen Gay will be providing direction and guidance concerning your inquiry about records retention/data storage policies and issues.

I'm sure we'll be working together more closely in the future.

Thanks for bringing up these important issues!

Regards,

Mariel Fox
Director, Records & Information Management
Museums, Archives & Rare Books (MARB)
LB 216 MD 1704
Direct: 470-578-2225
Main: 470-578-6289

----- Forwarded Message -----
From: "Jeff Milsteen" <jmilstee@kennesaw.edu>
To: "Steven Dean" <sdean29@kennesaw.edu>
Cc: "Mariel Fox" <mfox32@kennesaw.edu>
Sent: Friday, March 10, 2017 1:38:30 PM
Subject: Re: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Steven,

Mariel forwarded your inquiry to me. I believe there are a number of issues here that will require some additional work. For example, some of the data maintained by the Center is, by contract, property of the Secretary of State. That data would be subject to the Secretary of State's records retention policies and presumably those records should either be returned to the SOS Office or, if appropriate, destroyed at their direction and pursuant to their policies. All other records of the Center would be subject to the retention policies of KSU and Mariel can probably help you with existing retention guidelines. The trick, of course, is to correctly identify and categorize those records.

I was not clear what was being asked with respect to FOIA requests. If the Center receives any open records requests, those should immediately be forwarded to the Legal Division for review. The requests themselves, like all other official records of the university, are subjection to our retention guidelines.

I hope this helps. If you have additional questions, please let me know. Thanks.

Jeff Milsteen
Chief Legal Affairs Officer

----- Original Message -----
From: "Mariel Fox" <mfox32@kennesaw.edu>
To: "Jeff Milsteen" <jmilstee@kennesaw.edu>
Sent: Friday, March 10, 2017 9:26:22 AM
Subject: Fwd: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Jeff,

This request (see below) for advice came from Steven Dean (sdean29@kennesaw.edu), IT Systems Support at the Center for Election Systems.

I spoke to him on the phone concerning what types of records to keep and how long to keep them, directing him to the State of Georgia retention schedules on the Georgia Archives website.

As to his question about FOIA requests, I said that for KSU open records requests, those are handled by Legal Affairs. But for the Center's records, I did not know. I told him I would forward this question to you.

Please let me know if you have any questions, of if you have any suggestions on how to handle such inquiries in the future.

Thank you!

Mariel Fox
Director, Records & Information Management
Museums, Archives & Rare Books (MARB)
LB 216 MD 1704
Direct: 470-578-2225
Main: 470-578-6289

----- Forwarded Message -----
From: stevendean@kennesaw.edu
To: "records2go" <records2go@kennesaw.edu>
Sent: Thursday, March 9, 2017 1:58:52 PM
Subject: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Date Available for Consultation: No in-person consolation needed.

REQUESTED BY: Steven Dean Phone# 470-578-2120

Campus: Kennesaw
Department: Center for Election Systems
Office Location: House 3205

Advice requested for:
Myself and my supervisor or manager.

Need advice on:
['Which records do we need to keep?', 'How long do we need to keep records?', 'Do we need to keep both hard copy and digitial files?', 'What are our records responsibilities?', 'Topic not listed above. Describe in comments.']

Additional comments:
In writing new policies for data storage for the Center, I'd like to see your written policies for data storage periods as relating to FOIA requests.

Preferred communication method: Email.

From:	Stephen Craig Gay
To:	Steven Jay Dean; Jason Stephen Figueroa
Cc:	Christopher Michael Dehner; James Christopher Gaddis; Michael L. Barnes
Subject:	Fwd: Plan of action for the passing of data
Date:	Wednesday, March 22, 2017 6:27:33 PM
Importance:	High

Steven and Jason,

Please work with Christopher Dehner on this tomorrow, as this functionality is at the core of securely returning the data to the Secretary of State's Office. Chris will pull in additional ISO staff members as needed and I'll be available if any challenges or questions come up.

Thank you,

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: "Stephen C Gay" <sgay@kennesaw.edu>
To: mbeaver@sos.ga.gov
Cc: "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "Michael Barnes" <mbarne28@kennesaw.edu>
Sent: Wednesday, March 22, 2017 6:25:02 PM
Subject: Plan of action for the passing of data

Merritt,

Thank you for the conversation regarding the ExpressPoll file pickup and discussion on getting the processed data back to your office. Looking over my notes, I have the following plan of action from our discussion:

Objective: KSU will use the Secretary of State SFTP server to upload the data moving forward, after which members of your team will coordinate the distribution to the counties which require the data.

Tasks:
- Remove all users/rights with the current KSU folder on the Secretary of State SFTP Server and provision new accounts for specified users (Likely SDean, MFiguero, CDehner)
- Work with Chris Dehner, in the UITS Information Security Office, to share and validate SFTP certificate for server.
- Work with Chris Dehner and members of CES to develop process for file transfer, account password expiration, and archiving of file and associated password sharing
- Chris Dehner will work with Steven and Jason on selecting the archive software client, SFTP client and validating the functionality
- Test the clients and processes, and resolve any challenges.

If you could send me the contact information for James and Stephen on your team I will share with the team and ask that they connect 1st thing tomorrow. I don't want to be a roadblock to these tasks and progress, but will check-in on

the progress and will be available to assist as needed.

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

From: Stephen Craig Gay
To: Ware, William D. II (AT) (FBI)
Subject: Fwd: Request for data retrieval
Date: Wednesday, March 15, 2017 1:51:26 PM

Agent Ware,

We received the request below from the Center for Election Systems regarding data contained on the seized server which they do not have a backup of. What is the possibility of having the data extracted and us picking it up?

Thank you for your consideration of this request.
Stephen

----- Forwarded Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, March 15, 2017 1:41:25 PM
Subject: Request for data retrieval

Stephen,

As discussed earlier today, we would like to retrieve certain records from elections.kennesaw.edu that support our daily office activities, items such as inventory records, workflow databases used during our ballot building efforts, and operation manuals. These data are located in the cesuser user directory at /home/cesuser. We would like to retrieve the entire cesuser directory, if possible.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From:	Stephen Craig Gay
To:	Christopher Michael Dehner
Cc:	Davide Gaetano
Subject:	Infrastructure projects for CES
Date:	Monday, July 10, 2017 5:48:48 PM

Chris,

Speaking to Davide about the infrastructure surplus recommendations and I would like to divide the project into 2 phases, one focused on the surplus, switches, and APC's mentioned in the AAR; and the 2nd focused on the slightly longer plan to add environmental and log monitoring. If you could please connect with him on these projects, I would sincerely appreciate it and if I can assist in any way please let me know.

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

From:	Stephen Craig Gay
To:	Ware, William D. II (AT) (FBI)
Subject:	Investigative update
Date:	Monday, March 13, 2017 7:59:09 AM

Agent Ware,

Good Monday morning. I wanted to take a moment to reach out to ask for an update on the status of the investigation. If there is anything at all we can do to assist please let me know.

Thank you,
Stephen

Sent from Nine

March 3, 2017

Election-related files

elections.kennesaw.edu

The voting system and electronic pollbooks used in Georgia require files to be named in compliance with the application's requirements. As a consequence, many of the files will have identical names, but their contents vary by county.

Some of the pollbook related files will only contain voter registration values. These files are used to update the electors list, indicating voters who were issued ballots during advance/early voting. Other pollbook files will contain the state's entire electors list.

The folder names relate to the content contained within the files placed within the folders, back to the county to which they are assigned. We developed a folder for each county (159) and within each folder we placed files generated for that individual county.

Examples of files posted for a county to pull down:

./Appling County/Proof/Audio/Appling Audio.zip – This zip file contains audio files linked within the county's election database. This files are posted so a county can proof whether the candidate's name, ballot information headers, race headers are all present and recorded properly. The file is zipped due to file size.

./Appling County/Proof/Ballot/01 – Appling.zip – This zip file contains ballot proofs for a given election. These files are provided to each county to allow them to confirm that the contents of their ballots are accurate for the given election. The file is zipped due to files size.

./Appling County/Proof/Ballots/Ballot and Audio Proofs Signoff_v2.pdf – This file is provided to every county when proofing audio files and ballot proofs. We require each county to return a signed signoff form to our office after they have completed their proofing. This form allows the completed election database to be released from us to the jurisdiction for use in the given election. "V2" indicates that this is the second version of this form.

./Appling County/ExpressPoll/Numbered_List/001 (11-08-2016).pdf – This file is provided to every county after the completion of the given election. This file contains a list of those voters who participated at their assigned polling location on Election Day in sequential order.

./Appling County/ExpressPoll/ABSFile/PollData.db3 – This is a data file for use within the assigned county on their ExpressPoll units that are used to create voter access cards given to voters during the Advance Voting period. No individual voter data is contained within this file. A file of this nature is created for each county prior to a given election. "ABS" relates to voters casting ballots prior to Election Day.

./Appling County/ExpressPoll/ABSFile/Expoll.resources – This file accompanies the above mention file. The resource file instructs the ExpressPoll device what operations to allow and what buttons to display on screen to the user of the ExpressPoll device.

./Baldwin County/ExpressPoll/ED_Files/November 2016 General Voter Lookup.zip – This file is not built for all counties. This file is only built for those counties who request it from our office. This file contains the elector's list for the county for the given election, but it is not used to create any voter access cards. The file is zipped due to size of the files content.

./Baldwin County/ExpressPoll/ED_Files/November 2016 General Voter Lookup Password Memo.pdf – This file accompanies the above mentioned file. This file contains what the passwords are to access the data contained in the zipped file above when loaded onto an ExpressPoll. These passwords are changed for every election.

./Cherokee County/ExpressPoll/ED_Files/November2016GeneralElectionDay.zip – This is not a file posted for each county. This file is only posted to those counties who produce the storage media loaded into the jurisdictions' ExpressPolls themselves. Counties that do this operation are: Fulton, Cobb, Dekalb, Gwinnett, Forsyth, Chatham, Muscogee, Henry, Columbia, Clayton, and Cherokee. This file contains the full elector's list for the state for a given election.

./Cherokee County/ExpressPoll/ED_Files/November 2016 General Election Day Password Memo.pdf - This file accompanies the above mentioned file. This file contains what the passwords are to access the data contained in the zipped file above when loaded onto an ExpressPoll. These passwords are changed for every election.

./Clayton County/GEMS_DB/****.gbf – This is a file posted to a county only in select circumstances. This is an election database file containing the ballot contents for a given election. These files are accessed by the GEMS application.

./Pickens County/ExpressPoll/ED_Files/ExpReport.exe – File allows a county to produce a numbered list of voters directly from the ExpressPoll media, when installed on the ExpressPoll media.

./Pickens County/ExpressPoll/ED_Files/System.Data.SQLite.DLL – This file allows the file mentioned above to operate on the ExpressPoll. The above file is inoperative without this file.

./Richmond County/GEMS_DB/2. GEMS Instructions.pdf – This is a manual on GEMS operations. Only posted if requested by a county.

./Richmond County/GEMS_DB/GeneralDemo.zip – Only posted if requested by a county. Contains a demonstration election database.

This concludes the types of files placed within the county folders for distribution to counties

Attached is the known county user accounts allowing access to these to county folders. When an account is created, the county recipient is automatically sent (by Drupal) an email that contains a password reset link. Counties create their own passwords for accessing the folders.

Username	Folder	Phone Number
Appling County Elections	Appling County	912-367-8113
Appling County Registrar	Appling County	912-367-8113
Atkinson County Elections	Atkinson County	912-422-3003
Atkinson County Registrar	Atkinson County	912-422-3003
Bacon County Elections	Bacon County	912-632-5551
Bacon County Registrar	Bacon County	912-632-5551
Baker County Elections	Baker County	229-734-3019
Baker County Registrar	Baker County	229-734-3019
Baldwin County Elections	Baldwin County	478-445-4807
Baldwin County Registrar	Baldwin County	478-445-4807
Banks County Elections	Banks County	706-677-6260
Banks County Registrar	Banks County	706-677-6260
Barrow County Elections	Barrow County	770-307-3510
Barrow County Registrar	Barrow County	770-307-3510
Bartow County Elections	Bartow County	770-387-5098
Bartow County Registrar	Bartow County	770-387-5098
Ben Hill County Elections	Ben Hill County	229-426-5151
Ben Hill County Registrar	Ben Hill County	229-426-5151
Berrien County Elections	Berrien County	229-686-5213
Berrien County Registrar	Berrien County	229-686-5213
Bibb County Elections	Bibb County	478-621-6622
Bibb County Registrar	Bibb County	478-621-6622
Bleckley County Elections	Bleckley County	478-934-3204
Bleckley County Registrar	Bleckley County	478-934-3204
Brantley County Elections	Brantley County	912-462-6159
Brantley County Registrar	Brantley County	912-462-6159
Brooks County Elections	Brooks County	229-263-9939
Brooks County Registrar	Brooks County	229-263-9939
Bryan County Elections	Bryan County	912-653-3859
Bryan County Registrar	Bryan County	912-653-3859
Bulloch County Elections	Bulloch County	912-764-6502
Bulloch County Registrar	Bulloch County	912-764-6502
Burke County Elections	Burke County	770-775-8299
Burke County Registrar	Burke County	770-775-8299
Butts County Elections	Butts County	770-775-8299
Butts County Registrar	Butts County	770-775-8299

Calhoun County Elections	Calhoun County	229-849-2115
Calhoun County Registrar	Calhoun County	229-849-2115
Camden County Elections	Camden County	912-576-3785
Camden County Registrar	Camden County	912-576-3785
Candler County Elections	Candler County	912-515-4424
Candler County Registrar	Candler County	912-515-4424
Carroll County Elections	Carroll County	770-830-5824
Carroll County Registrar	Carroll County	770-830-5824
Catoosa County Elections	Catoosa County	706-935-3990
Catoosa County Registrar	Catoosa County	706-935-3990
Charlton County Elections	Charlton County	912-496-2607
Charlton County Registrar	Charlton County	912-496-2607
Chatham County Elections	Chatham County	912-201-4375
Chatham County Registrar	Chatham County	912-201-4375
Chattahoochee County Elections	Chattahoochee County	706-989-3603
Chattahoochee County Registrar	Chattahoochee County	706-989-3603
Chattooga County Elections	Chattooga County	706-857-0709
Chattooga County Registrar	Chattooga County	706-857-0709
Cherokee County Elections	Cherokee County	770-479-0407
Cherokee County Registrar	Cherokee County	770-479-0407
Clarke County Elections	Clarke County	706-613-3150
Clarke County Registrar	Clarke County	706-613-3150
Clay County Elections	Clay County	229-768-2445
Clay County Registrar	Clay County	229-768-2445
Clayton County Elections	Clayton County	770-477-4572
Clayton County Registrar	Clayton County	770-477-4572
Clinch County Elections	Clinch County	912-487-3656
Clinch County Registrar	Clinch County	912-487-3656
Cobb County Elections	Cobb County	770-528-2312
Cobb County Registrar	Cobb County	770-528-2312
Coffee County Elections	Coffee County	912-384-7018
Coffee County Registrar	Coffee County	912-384-7018
Colquitt County Elections	Colquitt County	229-616-7415
Colquitt County Registrar	Colquitt County	229-616-7415
Columbia County Elections	Columbia County	706-868-3355
Columbia County Registrar	Columbia County	706-868-3355
Cook County Elections	Cook County	229-896-7925
Cook County Registrar	Cook County	229-896-7925
Coweta County Elections	Coweta County	678-854-0015

Coweta County Registrar	Coweta County	678-854-0015
Crawford County Elections	Crawford County	478-836-1877
Crawford County Registrar	Crawford County	478-836-1877
Crisp County Elections	Crisp County	229-276-2611
Crisp County Registrar	Crisp County	229-276-2611
Dade County Elections	Dade County	706-657-8170
Dade County Registrar	Dade County	706-657-8170
Dawson County Elections	Dawson County	706-344-3640
Dawson County Registrar	Dawson County	706-344-3640
Decatur County Elections	Decatur County	229-243-2087
Decatur County Registrar	Decatur County	229-243-2087
DeKalb County Elections	DeKalb County	404-298-4020
DeKalb County Registrar	DeKalb County	404-298-4020
Dodge County Elections	Dodge County	478-374-3775
Dodge County Registrar	Dodge County	478-374-3775
Dooly County Elections	Dooly County	229-268-9023
Dooly County Registrar	Dooly County	229-268-9023
Dougherty County Elections	Dougherty County	229-431-3247
Dougherty County Registrar	Dougherty County	229-431-3247
Douglas County Elections	Douglas County	770-920-7412
Douglas County Registrar	Douglas County	770-920-7412
Early County Elections	Early County	229-723-4522
Early County Registrar	Early County	229-723-4522
Echols County Elections	Echols County	229-559-7526
Echols County Registrar	Echols County	229-559-7526
Effingham County Elections	Effingham County	912 754-8030
Effingham County Registrar	Effingham County	912 754-8030
Elbert County Elections	Elbert County	706-283-2016
Elbert County Registrar	Elbert County	706-283-2016
Emanuel County Elections	Emanuel County	478-237-3471
Emanuel County Registrar	Emanuel County	478-237-3471
Evans County Elections	Evans County	912-739-4080
Evans County Registrar	Evans County	912-739-4080
Fannin County Elections	Fannin County	706-632-7740
Fannin County Registrar	Fannin County	706-632-7740
Fayette County Elections	Fayette County	770-305-5138
Fayette County Registrar	Fayette County	770-305-5138
Floyd County Elections	Floyd County	706-291-5167
Floyd County Registrar	Floyd County	706-291-5167
Forsyth County Elections	Forsyth County	770-781-2118
Forsyth County Registrar	Forsyth County	770-781-2118

Franklin County Elections	Franklin County	706-384-4390
Franklin County Registrar	Franklin County	706-384-4390
Fulton County Elections	Fulton County	706-384-4390
Fulton County Registrar	Fulton County	706-384-4390
Gilmer County Elections	Gilmer County	706-635-4763
Gilmer County Registrar	Gilmer County	706-635-4763
Glascock County Elections	Glascock County	706-598-3241
Glascock County Registrar	Glascock County	706-598-3241
Glynn County Elections	Glynn County	912-554-7063
Glynn County Registrar	Glynn County	912-554-7063
Gordon County Elections	Gordon County	706-629-7781
Gordon County Registrar	Gordon County	706-629-7781
Grady County Elections	Grady County	229-377-4621
Grady County Registrar	Grady County	229-377-4621
Greene County Elections	Greene County	706-531-1108
Greene County Registrar	Greene County	706-531-1108
Gwinnett County Elections	Gwinnett County	678-226-7231
Gwinnett County Registrar	Gwinnett County	678-226-7231
Habersham County Elections	Habersham County	706-839-0170
Habersham County Registrar	Habersham County	706-839-0170
Hall County Elections	Hall County	770-531-6945
Hall County Registrar	Hall County	770-531-6945
Hancock County Elections	Hancock County	706-444-5259
Hancock County Registrar	Hancock County	706-444-5259
Haralson County Elections	Haralson County	770-646-2010
Haralson County Registrar	Haralson County	770-646-2010
Harris County Elections	Harris County	706-628-5210
Harris County Registrar	Harris County	706-628-5210
Hart County Elections	Hart County	706-376-8911
Hart County Registrar	Hart County	706-376-8911
Heard County Elections	Heard County	706-675-3353
Heard County Registrar	Heard County	706-675-3353
Henry County Elections	Henry County	770-288-6448
Henry County Registrar	Henry County	770-288-6448
Houston County Elections	Houston County	478-987-1973
Houston County Registrar	Houston County	478-987-1973
Irwin County Elections	Irwin County	229-468-5894
Irwin County Registrar	Irwin County	229-468-5894
Jackson County Elections	Jackson County	706-367-6377
Jackson County Registrar	Jackson County	706-367-6377
Jasper County Elections	Jasper County	706-468-4903

Jasper County Registrar	Jasper County	706-468-4903
Jeff Davis County Elections	Jeff Davis County	912-375-6635
Jeff Davis County Registrar	Jeff Davis County	912-375-6635
Jefferson County Elections	Jefferson County	478-625-8357
Jefferson County Registrar	Jefferson County	478-625-8357
Jenkins County Elections	Jenkins County	478-982-5581
Jenkins County Registrar	Jenkins County	478-982-5581
Johnson County Elections	Johnson County	478-864-4019
Johnson County Registrar	Johnson County	478-864-4019
Jones County Elections	Jones County	478-986-8234
Jones County Registrar	Jones County	478-986-8234
Lamar County Elections	Lamar County	770-358-5235
Lamar County Registrar	Lamar County	770-358-5235
Lanier County Elections	Lanier County	229-482-3668
Lanier County Registrar	Lanier County	229-482-3668
Laurens County Elections	Laurens County	478-272-2566
Laurens County Registrar	Laurens County	478-272-2566
Lee County Elections	Lee County	229-759-6002
Lee County Registrar	Lee County	229-759-6002
Liberty County Elections	Liberty County	912-876-3310
Liberty County Registrar	Liberty County	912-876-3310
Lincoln County Elections	Lincoln County	706-359-6126
Lincoln County Registrar	Lincoln County	706-359-6126
Long County Elections	Long County	912-545-2234
Long County Registrar	Long County	912-545-2234
Lowndes County Elections	Lowndes County	229-671-2850
Lowndes County Registrar	Lowndes County	229-671-2850
Lumpkin County Elections	Lumpkin County	706-864-6279
Lumpkin County Registrar	Lumpkin County	706-864-6279
Macon County Elections	Macon County	478-472-8520
Macon County Registrar	Macon County	478-472-8520
Madison County Elections	Madison County	706-795-6335
Madison County Registrar	Madison County	706-795-6335
Marion County Elections	Marion County	229-649-9838
Marion County Registrar	Marion County	229-649-9838
McDuffie County Elections	McDuffie County	706-595-2105
McDuffie County Registrar	McDuffie County	706-595-2105
McIntosh County Elections	McIntosh County	912-437-6605
McIntosh County Registrar	McIntosh County	912-437-6605
Meriwether County Elections	Meriwether County	706-672-9433
Meriwether County Registrar	Meriwether County	706-672-9433

Miller County Elections	Miller County	229-758-4110
Miller County Registrar	Miller County	229-758-4110
Mitchell County Elections	Mitchell County	229-336-2018
Mitchell County Registrar	Mitchell County	229-336-2018
Monroe County Elections	Monroe County	478-994-7036
Monroe County Registrar	Monroe County	478-994-7036
Montgomery County Elections	Montgomery County	912-583-2681
Montgomery County Registrar	Montgomery County	912-583-2681
Morgan County Elections	Morgan County	706-343-6311
Morgan County Registrar	Morgan County	706-343-6311
Murray County Elections	Murray County	706-517-1400 #7
Murray County Registrar	Murray County	706-517-1400 #7
Muscogee County Elections	Muscogee County	706-653-4392
Muscogee County Registrar	Muscogee County	706-653-4392
Newton County Elections	Newton County	678-625-1692
Newton County Registrar	Newton County	678-625-1692
Oconee County Elections	Oconee County	706-769-3958
Oconee County Registrar	Oconee County	706-769-3958
Oglethorpe County Elections	Oglethorpe County	706-743-5350
Oglethorpe County Registrar	Oglethorpe County	706-743-5350
Paulding County Elections	Paulding County	770-443-7503
Paulding County Registrar	Paulding County	770-443-7503
Peach County Elections	Peach County	478-825-3514
Peach County Registrar	Peach County	478-825-3514
Pickens County Elections	Pickens County	706-253-8781
Pickens County Registrar	Pickens County	706-253-8781
Pierce County Elections	Pierce County	912-449-2028
Pierce County Registrar	Pierce County	912-449-2028
Pike County Elections	Pike County	770-567-8734
Pike County Registrar	Pike County	770-567-8734
Polk County Elections	Polk County	770-749-2103
Polk County Registrar	Polk County	770-749-2103
Pulaski County Elections	Pulaski County	478-783-2061
Pulaski County Registrar	Pulaski County	478-783-2061
Putnam County Elections	Putnam County	706-485-8683
Putnam County Registrar	Putnam County	706-485-8683
Quitman County Elections	Quitman County	229-334-2224
Quitman County Registrar	Quitman County	229-334-2224
Rabun County Elections	Rabun County	706-782-1878
Rabun County Registrar	Rabun County	706-782-1878
Randolph County Elections	Randolph County	855-782-6310 ext 5

Randolph County Registrar	Randolph County	855-782-6310 ext 5
Richmond County Elections	Richmond County	706-821-2340
Richmond County Registrar	Richmond County	706-821-2340
Rockdale County Elections	Rockdale County	770-278-7333
Rockdale County Registrar	Rockdale County	770-278-7333
Schley County Elections	Schley County	229-937-2905
Schley County Registrar	Schley County	229-937-2905
Screven County Elections	Screven County	912-564-2783
Screven County Registrar	Screven County	912-564-2783
Seminole County Elections	Seminole County	229-524-5256
Seminole County Registrar	Seminole County	229-524-5256
Spalding County Elections	Spalding County	770-467-4370
Spalding County Registrar	Spalding County	770-467-4370
Stephens County Elections	Stephens County	706-886-8954
Stephens County Registrar	Stephens County	706-886-8954
Stewart County Elections	Stewart County	229-838-4682 ext 210
Stewart County Registrar	Stewart County	229-838-4682 ext 210
Sumter County Elections	Sumter County	229-928-4580
Sumter County Registrar	Sumter County	229-928-4580
Talbot County Elections	Talbot County	706-665-8270
Talbot County Registrar	Talbot County	706-665-8270
Taliaferro County Elections	Taliaferro County	706-456-2253
Taliaferro County Registrar	Taliaferro County	706-456-2253
Tattnall County Elections	Tattnall County	912-557-6417
Tattnall County Registrar	Tattnall County	912-557-6417
Taylor County Elections	Taylor County	478-862-3997
Taylor County Registrar	Taylor County	478-862-3997
Telfair County Elections	Telfair County	229-868-6038
Telfair County Registrar	Telfair County	229-868-6038
Terrell County Elections	Terrell County	229-995-5066
Terrell County Registrar	Terrell County	229-995-5066
Thomas County Elections	Thomas County	229-225-4101
Thomas County Registrar	Thomas County	229-225-4101
Tift County Elections	Tift County	229-386-7915
Tift County Registrar	Tift County	229-386-7915
Toombs County Elections	Toombs County	912-526-8226
Toombs County Registrar	Toombs County	912-526-8226
Towns County Elections	Towns County	706-896-6920
Towns County Registrar	Towns County	706-896-6920

Treutlen County Elections	Treutlen County	912-529-3342
Treutlen County Registrar	Treutlen County	912-529-3342
Troup County Elections	Troup County	706-883-1745
Troup County Registrar	Troup County	706-883-1745
Turner County Elections	Turner County	229-567-2909
Turner County Registrar	Turner County	229-567-2909
Twiggs County Elections	Twiggs County	478-945-3639
Twiggs County Registrar	Twiggs County	478-945-3639
Union County Elections	Union County	706-439-6041
Union County Registrar	Union County	706-439-6041
Upson County Elections	Upson County	706-647-6259
Upson County Registrar	Upson County	706-647-6259
Walker County Elections	Walker County	706-638-4349
Walker County Registrar	Walker County	706-638-4349
Walton County Elections	Walton County	770-267-1337
Walton County Registrar	Walton County	770-267-1337
Ware County Elections	Ware County	912-287-4363
Ware County Registrar	Ware County	912-287-4363
Warren County Elections	Warren County	706-465-2227
Warren County Registrar	Warren County	706-465-2227
Washington County Elections	Washington County	478-552-3304
Washington County Registrar	Washington County	478-552-3304
Wayne County Elections	Wayne County	912-427-5940
Wayne County Registrar	Wayne County	912-427-5940
Webster County Elections	Webster County	229-828-5775
Webster County Registrar	Webster County	229-828-5775
Wheeler County Elections	Wheeler County	912-568-7133
Wheeler County Registrar	Wheeler County	912-568-7133
White County Elections	White County	706-865-4141
White County Registrar	White County	706-865-4141
Whitfield County Elections	Whitfield County	706-278-7183
Whitfield County Registrar	Whitfield County	706-278-7183
Wilcox County Elections	Wilcox County	229-467-2111
Wilcox County Registrar	Wilcox County	229-467-2111
Wilkes County Elections	Wilkes County	706-678-2523
Wilkes County Registrar	Wilkes County	706-678-2523
Wilkinson County Elections	Wilkinson County	478-946-2188
Wilkinson County Registrar	Wilkinson County	478-946-2188
Worth County Elections	Worth County	229-776-8208
Worth County Registrar	Worth County	229-776-8208

From:	Steven Dean
To:	James Christopher Gaddis
Cc:	William C. Moore; Stephen Craig Gay; Michael L. Barnes; Merle Steven King
Subject:	Next steps for elections.kennesaw.edu
Date:	Thursday, March 2, 2017 1:32:27 PM

Chris, is there any further data you need from the server for your investigation? Our next intention is to make a backup of the affected files and remove them from the server. This would only affect files in the county folders, not log files are and config files. After that we will reach out to have the security of the server assessed by your group so that we may bring it back online without any previously vulnerable links.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

From: Stephen Craig Gay
To: mbeaver@sos.ga.gov
Cc: Lectra Lawhorne; Michael L. Barnes
Subject: Plan of action for the passing of data
Date: Wednesday, March 22, 2017 6:25:02 PM

Merritt,

Thank you for the conversation regarding the ExpressPoll file pickup and discussion on getting the processed data back to your office. Looking over my notes, I have the following plan of action from our discussion:

Objective: KSU will use the Secretary of State SFTP server to upload the data moving forward, after which members of your team will coordinate the distribution to the counties which require the data.

Tasks:
- Remove all users/rights with the current KSU folder on the Secretary of State SFTP Server and provision new accounts for specified users (Likely SDean, MFiguero, CDehner)
- Work with Chris Dehner, in the UITS Information Security Office, to share and validate SFTP certificate for server.
- Work with Chris Dehner and members of CES to develop process for file transfer, account password expiration, and archiving of file and associated password sharing
- Chris Dehner will work with Steven and Jason on selecting the archive software client, SFTP client and validating the functionality
- Test the clients and processes, and resolve any challenges.

If you could send me the contact information for James and Stephen on your team I will share with the team and ask that they connect 1st thing tomorrow. I don't want to be a roadblock to these tasks and progress, but will check-in on the progress and will be available to assist as needed.

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

From: Stephen Craig Gay
To: Steven Jay Dean
Cc: Michael L. Barnes; Christopher Michael Dehner
Subject: Question regarding private network
Date: Friday, June 23, 2017 7:24:59 AM

Steven,

Quick question: In preparation for next week's infrastructure meeting regarding the devices on the CES private network, I was curious how many of these devices allow for us to update or modify them? For example, the 16 Card Duplicators are likely dictated by the Secretary of State's Office and I would assume that there are other devices in this same scenario (GEMS server), but which devices could allow us to install local firewalls or run the latest version of operating software (Windows file server perhaps)?

Thanks,

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

From: Stephen Craig Gay
To: Michael L. Barnes
Subject: Re: Center for Election Systems Contract FY"17
Date: Tuesday, March 7, 2017 9:32:10 AM

Thanks Michael.

Stephen

Sent from Nine

From: Michael Barnes
Sent: Mar 7, 2017 8:57 AM
To: 'Stephen C. Gay'
Subject: Center for Election Systems Contract FY'17

Stephen,

Here is our current contract with the Secretary of State's office. The content of the contract hasn't really changed since 2012 or so.

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Christopher Dehner
To: Davide Gaetano
Cc: Casey Darrow; Stephen Gay; Chris Gaddis
Subject: RE: CES Network Assessment Meeting Notes 6/26
Date: Wednesday, July 19, 2017 1:29:00 PM
Attachments: CES Network surplus milestones.xlsx

Davide,

I think we're ready to make the final push on closing the CES AAR recommendations. All we have left is the imaging and transference of services of the two Dell PowerEdge R630s (both in CES private network data center) and the replacement of the UPSs. Per our conversations, one server is for DC/NAS and the other for Epic. I checked with Steven Dean and both servers not running any services so we can begin as soon as possible without impacting their services. The UPSs were ordered last week and we are waiting on delivery. I've included the project milestones and suggested due dates. If these due dates are not feasible, please provide alternative dates. If you have any questions, please feel free to reach out.

Regards,

Chris

From: Christopher Michael Dehner
Sent: Friday, July 7, 2017 11:16 AM
To: Davide Gaetano <dgaetano@students.kennesaw.edu>
Cc: Casey Darrow <cdarrow@kennesaw.edu>; Stephen Craig Gay <sgay@kennesaw.edu>; James Christopher Gaddis <jgaddis6@kennesaw.edu>
Subject: Fw: CES Network Assessment Meeting Notes 6/26

Davide,

I am reseeding this email because for some reason, it was sent to a dgaetano@students.kennesaw.edu account.

Per your instructions regarding the reimaging and installation of the CES server, we DBAN'd the hard drives and delivered the server to TS023. The server is a Dell PowerEdge R610 (Asset Tag: 103019). When it is ready for racking in the CES private network, please let me know and I'll coordinate with the Steven Dean.

Regards,

Chris

From: Christopher Michael Dehner
Sent: Tuesday, June 27, 2017 5:22 PM
To: Stephen Craig Gay; Nickolaus E Hassis; Jason Stephen Figueroa; Steven Jay Dean; Michael L. Barnes; Davide F Gaetano
Subject: CES Network Assessment Meeting Notes 6/26

CES Network Assessment
6/27/17 4:00PM-5:15PM
Attendees:
Nick Hassis, Stephen Gay, Jason Figuero, Steven Dean, Michael Barns, Davide Gaetano

Notes:

CES – is most secure network at KSU, making it more secure
9/10 AAR items closed - Final item: Private Network Inventory

Goal: Reduce number of devices on private network

IMI Card Duplicators also act as data extractor to private network NAS

Reconciled Windows XP devices not captured by network scan

GEMS services dependent on .NET version found on WinXP

Davide – Can GEMS services be virtualized to work on Win7 or Win10?
Steven – Not certain

Stephen: Can we use local authentication instead of domain controller?
Davide: Put domain controllers on Epic and NA

Cellular dialer to send syslog, environment, arpwatch alerts & GPS updates for time keeping.
New Epic and New NAS servicers will also be domain controllers
Cycle hard drive backups to fireproof safe in Secure Storage

Davide suggestions:
- Physically label computers if on private network
- Add distance between private and public network devices
- Replace wifi access point, create new ssid for only CES
- Arpwatch box for public and private networks to prevent network crossovers
- Put CES behind a firewall – force denial and whitelist

Action Items:

CES IT
- Confirm printer has unnecessary services disabled
- Work with vendor on upgrading Epic to more current version of Windows Server

UITS
- Build new XP image
- Windows 10 build for audio box

- Migrate data from Poweredge 1900 to Server TBD and decommission box
- Spin up new servers
- Collaborate with CES on transferring services to new servers
- Chris: Connect with Jonathan on new APCs
- Chris: Wipe R610 server, deliver to Davide & Casey for install
- Chris Schedule update meetings for CES Network Updates (include Casey, Jonathan, and GJ)

Christopher Dehner, CISA
IT Security Professional III
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 027
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: 470-578-6620
Fax: 470-578-9050
cmd9090@kennesaw.edu

From: Christopher Dehner
To: Stephen Gay
Cc: Michael Barnes; Steven Dean; Jason Figueroa
Subject: Re: CES server surplus
Date: Wednesday, August 9, 2017 3:54:39 PM

Stephen,

I'm happy to report that the remaining two servers on the AAR were delivered to ITIM and the hard drives were degaussed three times. Additionally, I followed up with Jonathan on replacing the old UPSs with the new ones.

Regards,

Chris

From: Stephen Gay
Sent: Wednesday, August 9, 2017 11:32 AM
To: Christopher Dehner; Steven Dean; Jason Figueroa
Cc: Michael Barnes; Lectra Lawhorne
Subject: Re: CES server surplus

Chris,

This is fantastic news. Great work to all parties on closing the final recommendation from the incident after action report.

In your service,
Stephen.

Sent from Nine

From: Christopher Dehner
Sent: Aug 9, 2017 11:24 AM
To: Steven Dean; Jason Figueroa
Cc: Michael Barnes; Stephen Gay
Subject: CES server surplus

Fellas,

I will arrive at the center around 1:30 today to pick up the old DC. I will also get the old unicoi server from secure storage. Additionally, I sent in a service ticket for this request.

Regards,

Chris

Get Outlook for Android

From: Stephen Gay
To: Christopher Dehner; Steven Dean; Jason Figueroa
Cc: Michael Barnes; Lectra Lawhorne
Subject: Re: CES server surplus
Date: Wednesday, August 9, 2017 11:32:38 AM

Chris,

This is fantastic news. Great work to all parties on closing the final recommendation from the incident after action report.

In your service,
Stephen.

Sent from Nine

From: Christopher Dehner
Sent: Aug 9, 2017 11:24 AM
To: Steven Dean; Jason Figueroa
Cc: Michael Barnes; Stephen Gay
Subject: CES server surplus

Fellas,

I will arrive at the center around 1:30 today to pick up the old DC. I will also get the old unicoi server from secure storage. Additionally, I sent in a service ticket for this request.

Regards,

Chris

Get Outlook for Android

From: Steven Dean
To: Mariel Louise Fox
Cc: Steven Jay Dean; Stephen Craig Gay
Subject: Re: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus
Date: Wednesday, March 15, 2017 4:31:54 PM

Thank you for your time the other day, Mariel, it was very helpful. I look forward to speaking again about this soon.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Mar 15, 2017, at 4:27 PM, Mariel Fox <mfox32@kennesaw.edu> wrote:

> Steven,
>
> I just learned that Stephen Gay will be providing direction and guidance concerning your inquiry about records retention/data storage policies and issues.
>
> I'm sure we'll be working together more closely in the future.
>
> Thanks for bringing up these important issues!
>
> Regards,
>
> Mariel Fox
> Director, Records & Information Management
> Museums, Archives & Rare Books (MARB)
> LB 216 MD 1704
> Direct: 470-578-2225
> Main: 470-578-6289
>
> ----- Forwarded Message -----
> From: "Jeff Milsteen" <jmilstee@kennesaw.edu>
> To: "Steven Dean" <sdean29@kennesaw.edu>
> Cc: "Mariel Fox" <mfox32@kennesaw.edu>
> Sent: Friday, March 10, 2017 1:38:30 PM
> Subject: Re: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus
>
> Steven,
>
> Mariel forwarded your inquiry to me. I believe there are a number of issues here that will require some additional work. For example, some of the data maintained by the Center is, by contract, property of the Secretary of State. That data would be subject to the Secretary of State's records retention policies and presumably

those records should either be returned to the SOS Office or, if appropriate, destroyed at their direction and pursuant to their policies. All other records of the Center would be subject to the retention policies of KSU and Mariel can probably help you with existing retention guidelines. The trick, of course, is to correctly identify and categorize those records.

I was not clear what was being asked with respect to FOIA requests. If the Center receives any open records requests, those should immediately be forwarded to the Legal Division for review. The requests themselves, like all other official records of the university, are subjection to our retention guidelines.

I hope this helps. If you have additional questions, please let me know. Thanks.

Jeff Milsteen
Chief Legal Affairs Officer

----- Original Message -----
From: "Mariel Fox" <mfox32@kennesaw.edu>
To: "Jeff Milsteen" <jmilstee@kennesaw.edu>
Sent: Friday, March 10, 2017 9:26:22 AM
Subject: Fwd: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Jeff,

This request (see below) for advice came from Steven Dean (sdean29@kennesaw.edu), IT Systems Support at the Center for Election Systems.

I spoke to him on the phone concerning what types of records to keep and how long to keep them, directing him to the State of Georgia retention schedules on the Georgia Archives website.

As to his question about FOIA requests, I said that for KSU open records requests, those are handled by Legal Affairs. But for the Center's records, I did not know. I told him I would forward this question to you.

Please let me know if you have any questions, of if you have any suggestions on how to handle such inquiries in the future.

Thank you!

Mariel Fox
Director, Records & Information Management
Museums, Archives & Rare Books (MARB)
LB 216 MD 1704
Direct: 470-578-2225
Main: 470-578-6289

----- Forwarded Message -----
From: stevendean@kennesaw.edu
To: "records2go" <records2go@kennesaw.edu>
Sent: Thursday, March 9, 2017 1:58:52 PM
Subject: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Date Available for Consultation: No in-person consolation needed.

REQUESTED BY: Steven Dean Phone# 470-578-2120

Campus: Kennesaw
Department: Center for Election Systems
Office Location: House 3205

Advice requested for:
Myself and my supervisor or manager.

Need advice on:
['Which records do we need to keep?', 'How long do we need to keep records?', 'Do we need to keep both hard copy and digitial files?', 'What are our records responsibilities?', 'Topic not listed above. Describe in comments.']

Additional comments:
In writing new policies for data storage for the Center, I'd like to see your written policies for data storage periods as relating to FOIA requests.

Preferred communication method: Email.

From: Ware, William D. II (AT) (FBI)
To: Stephen Craig Gay
Subject: RE: Investigative update
Date: Tuesday, March 14, 2017 9:02:53 AM

Hi Stephen,

Sorry for the late reply. The investigation is moving along. We are reviewing the logs and issuing legal process. The legal process is what will take the longest. It could take from two weeks to a month depending on the Internet Service Provider.

Thanks,
SA Davey Ware
FBI - Atlanta Division
2635 Century Parkway, NE
Suite 400
Atlanta, GA
O: 404-679-6126
C: 404-520-3342
F: 404-679-1417

From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Monday, March 13, 2017 7:59 AM
To: Ware, William D. II (AT) (FBI) <William.Ware@ic.fbi.gov>
Subject: Investigative update

Agent Ware,

Good Monday morning. I wanted to take a moment to reach out to ask for an update on the status of the investigation. If there is anything at all we can do to assist please let me know.

Thank you,
Stephen

Sent from Nine

From: Koonce, Steven
To: Christopher Michael Dehner
Cc: Oliver, James; Stephen Craig Gay; Steven Jay Dean; Jason Stephen Figueroa; James Christopher Gaddis
Subject: RE: KSU Account Creation and SFTP Key Management
Date: Friday, March 24, 2017 11:47:05 AM

Our current FTP server uses FTPS (also known as FTP with SSL). Whether we remain on the existing server or stand up a new server, the FTP accounts we are setting up will use a secure protocol, most likely FTPS.

-----Original Message-----
From: Christopher M. Dehner [mailto:cmd9090@kennesaw.edu]
Sent: Friday, March 24, 2017 11:42 AM
To: Koonce, Steven <skoonce@sos.ga.gov>
Cc: Oliver, James <Joliver@sos.ga.gov>; sgay <sgay@kennesaw.edu>; Steven Dean <sdean29@kennesaw.edu>; Jason Figueroa <jfigue12@kennesaw.edu>; jgaddis6 <jgaddis6@kennesaw.edu>
Subject: Re: KSU Account Creation and SFTP Key Management

Steven,

Just a quick point of clarification, when referring to FTP in your email, are you including SFTP or FTPS in your conversations? Per USG Policy and information security best practices, KSU don't allow straight FTP transfers. External file transfers are managed through SFTP or FTPS. Can you confirm that we'll be using SFTP or FTPS to manage these transfers.

Regards,

Christopher Dehner, CISA
IT Security Professional III
Information Security Office
University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 027
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: 470-578-6620
Fax: 470-578-9050
cmd9090@kennesaw.edu

----- Original Message -----
From: "Koonce, Steven" <skoonce@sos.ga.gov>
To: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
Cc: "Oliver, James" <Joliver@sos.ga.gov>, "sgay" <sgay@kennesaw.edu>, "Steven Dean" <sdean29@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "jgaddis6" <jgaddis6@kennesaw.edu>
Sent: Friday, March 24, 2017 11:33:01 AM
Subject: RE: KSU Account Creation and SFTP Key Management

We are having an Internal IT meeting Monday to review governance of our FTP site and to decide if a separate FTP server will be used for Elections processes.

I am going to work on the accounts below this afternoon so that they will be ready to go on Monday provided we have no significant changes in our FTP Infrastructure.

-----Original Message-----
From: Christopher M. Dehner [mailto:cmd9090@kennesaw.edu]
Sent: Friday, March 24, 2017 11:23 AM

To: Koonce, Steven <skoonce@sos.ga.gov>
Cc: Oliver, James <Joliver@sos.ga.gov>; Stephen C. Gay <sgay@kennesaw.edu>; Steven Dean <sdean29@kennesaw.edu>; Jason Figueroa <jfigue12@kennesaw.edu>; Chris Gaddis <jgaddis6@kennesaw.edu>
Subject: KSU Account Creation and SFTP Key Management

Steven,

My name is Christopher Dehner and I work in the KSU Information Security Office. I've been tasked to cooridnate with you on creating accounts for KSU Center for Elections Systems technicians in the Secretary of State's SFTP server. We would like the following users added:

Steven Dean
Jason Figueroa
Christopher Dehner

I would like to have my account disabled but still in the system. This will allow us to reactivate the account if my support is needed. Additionally, are you able to accommodate specific password requirements (length, special characters, annual expiration, etc.). If at all possible, we would like to align it with our institutional practices. If not, we can discuss this further.

After the accounts are provisioned but before any data transfers, we would like to validate the SFTP encryption key. Based on our understanding, we'll need to make a connection and have you provide the key which we can validate against the SFTP client. This would probably be best done over the phone. If you have an alternative method of key validation, we'll be happy to discuss.

We're looking forward to patterning with your office in building secures processes for data transfers. If you have any additional questions, comments, or concerns, please feel free to reach out.

Warmest Regards,

Christopher Dehner, CISA
IT Security Professional III
Information Security Office
University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 027
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: 470-578-6620
Fax: 470-578-9050
cmd9090@kennesaw.edu

From: Christopher Michael Dehner
To: Casey Darrow
Cc: Stephen Craig Gay; Chase Alexander Elliott; Freddie Lewis
Subject: Re: New server and share
Date: Tuesday, March 21, 2017 3:09:44 PM

Casey,

We would like this only accessible on-campus from the following subnet:

10.62.44.0/24 (House 57)

Additionally, we would like all off-campus traffic prohibited. If you need anything else, just let me know.

Regards,

Christopher Dehner, CISA
IT Security Professional III
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 027
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: 470-578-6620
Fax: 470-578-9050
cmd9090@kennesaw.edu

----- Original Message -----
From: "Casey Darrow" <cdarrow@kennesaw.edu>
To: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
Cc: "sgay" <sgay@kennesaw.edu>, "Chase Elliott" <celliot7@kennesaw.edu>, "Freddie Lewis" <flewis15@kennesaw.edu>
Sent: Tuesday, March 21, 2017 2:44:04 PM
Subject: Re: New server and share

Thanks!

Casey Darrow
Director of Windows Server and Infrastructure
University Information Technology Services
Kennesaw State University
Phone 470-578-2634

From: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
To: "cdarrow" <cdarrow@kennesaw.edu>
Cc: "Stephen C Gay" <sgay@kennesaw.edu>, "Chase Elliott" <celliot7@kennesaw.edu>, "Freddie Lewis" <flewis15@kennesaw.edu>
Sent: Tuesday, March 21, 2017 2:43:28 PM
Subject: Re: New server and share

Casey,

I'll co-ordinate with CFES technicians, let me gather that information and get back to you.

Christopher Dehner, CISA
IT Security Professional III
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 027
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: 470-578-6620
Fax: 470-578-9050
cmd9090@kennesaw.edu

----- Original Message -----
From: "Casey Darrow" <cdarrow@kennesaw.edu>
To: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
Cc: "sgay" <sgay@kennesaw.edu>, "Chase Elliott" <celliot7@kennesaw.edu>, "Freddie Lewis" <flewis15@kennesaw.edu>
Sent: Tuesday, March 21, 2017 2:37:47 PM
Subject: Re: New server and share

Chris,

Can you get us the firewall rules we that are needed? We just need to know what exact IP or what subnets need to access this fileshare. Or should we work directly with Steven Dean on this?

Thanks,
Casey

Casey Darrow
Director of Windows Server and Infrastructure
University Information Technology Services
Kennesaw State University
Phone 470-578-2634

From: "Stephen C Gay" <sgay@kennesaw.edu>
To: "Steven Dean" <stevendean@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "Christopher M. Dehner" <cmd9090@kennesaw.edu>, "Chase Elliott" <celliot7@kennesaw.edu>, "cdarrow" <cdarrow@kennesaw.edu>
Sent: Tuesday, March 21, 2017 11:14:06 AM
Subject: Re: New server and share

Steven,

I would like for us to have all safeguards in place before CES begins using the server in a production sense. Chris Dehner is CC'd on this email and, by copy, I'll ask him to coordinate between the WinServ team and CES on making this a priority

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

----- Original Message -----
From: "Steven Dean" <stevendean@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>, "Elliott Chase" <celliot7@kennesaw.edu>, "Casey Darrow" <cdarrow@kennesaw.edu>
Sent: Tuesday, March 21, 2017 11:04:04 AM
Subject: Re: New server and share

Stephen, thank you. Can we begin using this share today to host our project tracker and inventory lists? Or do we need to wait for the firewall changes?

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Mar 21, 2017, at 7:44 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven and Jason,
>
> The WinServ team has provisioned a new server dedicated to CES and created a file share which is locked down to the list of users in the center. The path to the share is
>
> \\FS-ES.kennesaw.edu\shared
>
> As we discussed on Friday, I'd like to use a host-based firewall on the server to only allow traffic from the CES network and the UITS network (for management). As I get more information I'll pass along.
>
> Stephen

From: Beaver, Merritt
To: Stephen Craig Gay; Koonce, Steven; Oliver, James
Cc: Lectra Lawhorne; Michael L. Barnes
Subject: RE: Plan of action for the passing of data
Date: Thursday, March 23, 2017 10:24:00 AM

Stephen

I would like to tie in both Steven Koonce, one of our Network administrators and James Oliver, our security manager. See their emails attached.

I talked with my team and our election's team and we would like to just create a new set of SFTP folders for this effort. The old folder was set up the exchange sample ballot forms and we would like to not repurpose that folder for this new use. There will be a need for KSU to upload files to SOS and also for SOS to send files to KSU. We are suggesting that we have two folders to serve each of these purposes. Both of these folders will only hold data for 30 days and after that time any files left will be automatically deleted as these will be transfer folders only.

I will let Steven and James work with your team to best set this environment up.

Thanks

Merritt

S. Merritt Beaver
Chief Information Officer
Office of Georgia Secretary of State Brian P. Kemp
Office (404) 656-7744 Mobile: (770)330-0016
mbeaver@sos.ga.gov

-----Original Message-----
From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Wednesday, March 22, 2017 6:25 PM
To: Beaver, Merritt <mbeaver@sos.ga.gov>
Cc: Lectra Lawhorne <llawhorn@kennesaw.edu>; Michael Barnes <mbarne28@kennesaw.edu>
Subject: Plan of action for the passing of data

Merritt,

Thank you for the conversation regarding the ExpressPoll file pickup and discussion on getting the processed data back to your office. Looking over my notes, I have the following plan of action from our discussion:

Objective: KSU will use the Secretary of State SFTP server to upload the data moving forward, after which members of your team will coordinate the distribution to the counties which require the data.

Tasks:
- Remove all users/rights with the current KSU folder on the Secretary of State SFTP Server and provision new accounts for specified users (Likely SDean, MFiguero, CDehner)
- Work with Chris Dehner, in the UITS Information Security Office, to share and validate SFTP certificate for server.
- Work with Chris Dehner and members of CES to develop process for file transfer, account password expiration, and archiving of file and associated password sharing
- Chris Dehner will work with Steven and Jason on selecting the archive software client, SFTP client and validating the functionality
- Test the clients and processes, and resolve any challenges.

If you could send me the contact information for James and Stephen on your team I will share with the team and ask that they connect 1st thing tomorrow. I don't want to be a roadblock to these tasks and progress, but will check-in on the progress and will be available to assist as needed.

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

From: Michael L. Barnes
To: Stephen Craig Gay
Subject: Re: Plan of action for the passing of data
Date: Wednesday, March 22, 2017 6:26:57 PM

Thank you jumping on this quickly.

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

On Mar 22, 2017, at 6:25 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:

> Merritt,
>
> Thank you for the conversation regarding the ExpressPoll file pickup and discussion on getting the processed data back to your office. Looking over my notes, I have the following plan of action from our discussion:
>
> Objective: KSU will use the Secretary of State SFTP server to upload the data moving forward, after which members of your team will coordinate the distribution to the counties which require the data.
>
> Tasks:
> - Remove all users/rights with the current KSU folder on the Secretary of State SFTP Server and provision new accounts for specified users (Likely SDean, MFiguero, CDehner)
> - Work with Chris Dehner, in the UITS Information Security Office, to share and validate SFTP certificate for server.
> - Work with Chris Dehner and members of CES to develop process for file transfer, account password expiration, and archiving of file and associated password sharing
> - Chris Dehner will work with Steven and Jason on selecting the archive software client, SFTP client and validating the functionality
> - Test the clients and processes, and resolve any challenges.
>
> If you could send me the contact information for James and Stephen on your team I will share with the team and ask that they connect 1st thing tomorrow. I don't want to be a roadblock to these tasks and progress, but will check-in on the progress and will be available to assist as needed.
>
> 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

From: Michael L. Barnes
To: Christopher Michael Dehner
Cc: Steven Jay Dean; Stephen Craig Gay
Subject: Re: Question
Date: Wednesday, March 29, 2017 12:10:55 PM

Will do.

Thank you.

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

On Mar 29, 2017, at 12:10 PM, Christopher M. Dehner <cmd9090@kennesaw.edu> wrote:

> Michael,
>
> From a security perspective we don't have an issue with sending a sample ballot via email, as it contains no confidential data. I would advise to double check with the SoS investigator that this is their preferred method of transmission. As we continue to collaborate with the SoS IT department, we can standardize and document these processes.
>
> Regards,
>
> ---
> Christopher Dehner, CISA
> IT Security Professional III
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 027
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: 470-578-6620
> Fax: 470-578-9050
> cmd9090@kennesaw.edu
>
> ----- Original Message -----
> From: "Michael Barnes" <mbarne28@kennesaw.edu>
> To: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
> Cc: "Steven Dean" <sdean29@kennesaw.edu>
> Sent: Wednesday, March 29, 2017 11:12:29 AM
> Subject: Question

EXHIBIT 2

From: **Merle S. King** mking@kennesaw.edu
Subject: Re: PII found on unicoi.kennesaw.edu (only open to the KSU network)
Date: March 4, 2017 at 6:17 PM
To: Lectra Lawhorne llawhorn@kennesaw.edu
Cc: Stephen C. Gay sgay@kennesaw.edu, Michael Barnes mbarne28@kennesaw.edu, sdean29@kennesaw.edu

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 Pl
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

Michael Barnes

From: Stephen Craig Gay
Sent: Saturday, March 04, 2017 5:49 PM
To: Michael L. Barnes
Cc: Lectra Lawhorne; Merle Steven King
Subject: Fw: PII found on unicoi.kennesaw.edu (only open to the KSU network)

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 Pl
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

Michael Barnes

From:	Merle Steven King
Sent:	Sunday, August 28, 2016 3:56 PM
To:	Steven Jay Dean; Jason Stephen Figueroa
Cc:	Michael L. Barnes
Subject:	Fwd: [IMPORTANT] concerning the security of elections.kennesaw.edu

Steven and Jason - Please review this email and advise. Sooner is better than later.

Thanks,

MSK

From: "Logan Lamb"
To: "Merle King"
Cc: research@bastille.net
Sent: Sunday, August 28, 2016 3:47:50 PM
Subject: [IMPORTANT] concerning the security of elections.kennesaw.edu

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

--

Merle S. King

Executive Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, Georgia 30144

Voice: 470-578-6900
Fax: 470-578-9012

Michael Barnes

From:	Merle Steven King
Sent:	Wednesday, March 01, 2017 11:45 PM
To:	Michael L. Barnes; Steven Jay Dean
Subject:	Fwd: Vulnerability on the elections.kennesaw.edu website

FYI.

Sent from my iPad

Begin forwarded message:

> **From:** "Stephen C. Gay" <sgay@kennesaw.edu>
> **Date:** March 1, 2017 at 11:10:16 PM EST
> **To:** Merle King <mking@kennesaw.edu>, Steven Dean <sdean29@kennesaw.edu>
> **Cc:** Lectra Lawhorne <llawhorn@kennesaw.edu>, "William C. Moore" <wmoore36@kennesaw.edu>
> **Subject: Fwd: Vulnerability on the elections.kennesaw.edu website**
>
> 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

Michael Barnes

From: Steven Dean <stevendean@kennesaw.edu>
Sent: Thursday, March 02, 2017 1:32 PM
To: James Christopher Gaddis
Cc: William C. Moore; Stephen Craig Gay; Michael L. Barnes; Merle Steven King
Subject: Next steps for elections.kennesaw.edu

Chris, is there any further data you need from the server for your investigation? Our next intention is to make a backup of the affected files and remove them from the server. This would only affect files in the county folders, not log files are and config files. After that we will reach out to have the security of the server assessed by your group so that we may bring it back online without any previously vulnerable links.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

Michael Barnes

From: Steven Jay Dean
Sent: Wednesday, April 26, 2017 3:18 PM
To: Christopher Michael Dehner
Cc: Merle Steven King; Michael L. Barnes; Jason Stephen Figueroa
Subject: Private Network Hardware Assessment

Chris, we recently receive a draft of the Incident report and I would like to go through the hardware section to get a plan outlined for addressing the recommendations. The document states the following:

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 – Electors list creation box
   Recommendation: Continue as ISO/CES managed
6. EPIC Files – Dell 1900 – Age 6+ years – Electors list creation box 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

We had submitted for approval to UITS the purchase of two new UPS units prior to the incident. Should we continue and order these as previously planned?
Will new hardware (and other equipment) be ordered by ISO under ISO budget, ordered by ISO under CES budget, or ordered by CES? Who will decide what hardware is purchased?
How should we proceed with replacing the Switches and who will install and manage them?
When will the assessment of the private network software commence and what department will handle the migrations and updates? How will this project factor into their schedule?

We would like to get moving on this list as soon as possible. Please let me know what I can do as the next step. Thanks.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road

Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

Michael Barnes

From: Merle Steven King
Sent: Monday, August 29, 2016 11:06 AM
To: Michael L. Barnes
Subject: Re: Follow Up from earlier email regarding security of elections.kennesaw.edu

Well said. Thanks

--

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 Aug 29, 2016, at 11:04 AM, Michael Barnes <mbarne28@kennesaw.edu> wrote:

> Stephen,
> In retrospect, I need to pull back my request that you include Logan Lamb or his associated organization Bastille Threat Research Team (www.bastille.net) on a black list of ip addresses. My request was an over-reaction on my part. The quick security assessment they provided us, though unsolicited, did highlight an issue we needed to resolve with our website. To black list them for helping us would be inappropriate.
> Leading up to this election, where the question of whether or not someone can hack election systems is so in the forefront, we will need your team will help us continually analyze our online systems and inspect for any openings that need to be sealed. Our IT staff will be in touch today to let you know what enhancements we have made and will request that your team ping our system to see if you all find other issues.
> Thanks in advance for your help,
> Michael Barnes
> Director
> Center for Election Systems
> Kennesaw State University
> 3205 Campus Loop Road
> Kennesaw, GA 30144
> ph: 470-KSU-6900
> fax: 470-KSU-9012

Michael Barnes

From: Stephen Craig Gay
Sent: Thursday, April 27, 2017 10:29 AM
To: Michael L. Barnes; Merle Steven King
Cc: Lectra Lawhorne; Christopher Michael Dehner
Subject: Re: Incident Reponse Walk through
Attachments: CES AAR Rev04.pdf

Michael and Merle,

Thank you for the edits. I have accepted them and attached the updated version and will be on the lookout for the referenced email.

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

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, April 26, 2017 3:29:43 PM
Subject: RE: Incident Reponse Walk through

Stephen,

Thank you for giving us the opportunity to review the attached. We have provided a few grammatical changes and added just a few clarifying comments.
I am attaching a copy with Change Tracker on so you can quickly see those changes.

We have asked Steven Dean to follow up with Chris Dehner to see what timeline may be in place in relation to items listed in Issue 7. We want to make sure we are doing our part but we will need some guidance.

Please let us know what other assistance we can provide.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144

ph: 470-KSU-6900
fax: 470-KSU-9012
-----Original Message-----
From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Monday, April 24, 2017 12:01 PM
To: Merle King <mking@kennesaw.edu>; Michael Barnes <mbarne28@kennesaw.edu>
Cc: Lectra Lawhorne <llawhorn@kennesaw.edu>; Christopher M. Dehner <cmd9090@kennesaw.edu>
Subject: Re: Incident Reponse Walk through

Merle & Michael,

Following up on this, one of the areas in which we are actively looking to grow is in the "Post-Incident Activity" area and specifically working to understand what vectors led to a compromise and what KSU could have done better to close those vectors (or minimally detected earlier). For the Center for Election Systems incident, we adopted a format which GaTech shared to conduct document incident "After Action Reports". The document purposely vague in regards to the incident, but is highly tactical in prescribing mitigation steps to prevent future incidents.

Can I ask you to review and provide your feedback, as I value your input and all mitigation is going to be conducted in a secure and collaborative manner.

Thank you,
Stephen

----- Original Message -----
From: "Merle King" <mking@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "Steven Dean" <sdean29@kennesaw.edu>
Sent: Tuesday, April 18, 2017 9:55:05 AM
Subject: Incident Reponse Walk through

Stephen - We are looking for assistance in designing and conducting an incident response exercise walk through for several difference scenarios here at the Center. Do you have a template or other guidelines that can help us organize the exercise? We would like to include our staff, UITS, and SOS IT staff in the exercise.

Thanks in advance,

Merle

--
Merle S. King

Executive Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, Georgia 30144

Voice: 470-578-6900
Fax: 470-578-9012

Michael Barnes

From: James Christopher Gaddis
Sent: Thursday, March 02, 2017 1:59 PM
To: Steven Dean
Cc: William C. Moore; Stephen Craig Gay; Michael L. Barnes; Merle Steven King
Subject: Re: Next steps for elections.kennesaw.edu

Steven,

As long as all log and config files are kept and you keep a record of what actions you are taking then I have no problem with that. We SHOULD have everything we need but you never know what questions might come up based upon the data we are reviewing.

Thanks,

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

----- Original Message -----
From: "Steven Dean" <stevendean@kennesaw.edu>
To: "Chris Gaddis" <jgaddis6@kennesaw.edu>
Cc: "William C. Moore" <wcmoore@kennesaw.edu>, "Stephen C Gay" <sgay@kennesaw.edu>, "Michael Barnes" <mbarne28@kennesaw.edu>, "Merle S. King" <mking@kennesaw.edu>
Sent: Thursday, March 2, 2017 1:32:15 PM
Subject: Next steps for elections.kennesaw.edu

Chris, is there any further data you need from the server for your investigation? Our next intention is to make a backup of the affected files and remove them from the server. This would only affect files in the county folders, not log files are and config files. After that we will reach out to have the security of the server assessed by your group so that we may bring it back online without any previously vulnerable links.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

Michael Barnes

From: Stephen Craig Gay
Sent: Saturday, March 04, 2017 7:42 PM
To: Michael L. Barnes
Cc: Lectra Lawhorne; Merle Steven King
Subject: Re: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Michael,

Thank you so much and appreciate you coming to KSU to handle this tonight.

Stephen

Sent from Nine

From: Michael Barnes
Sent: Mar 4, 2017 7:11 PM
To: Stephen C. Gay
Cc: Lectra Lawhorne; Merle King
Subject: Re: PII found on unicoi.kennesaw.edu (only open to the KSU network)

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 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 Pl
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

Michael Barnes

From: Stephen Craig Gay
Sent: Thursday, May 04, 2017 10:08 AM
To: Michael L. Barnes
Cc: Lectra Lawhorne; Christopher Michael Dehner; Merle Steven King
Subject: Re: Private Network Hardware Assessment

Michael,

Thank you for forwarding the email. UITS, as the provider of network infrastructure & connectivity, will provide the funding and specs for the battery backups as well as replacement switches. Other IT equipment which is specific to CES's mission (desktops/servers on the isolated network) will continue to be funded from the Center's budget and we will all work together on hardware specs which allows for support/maintenance to align with KSU standards.

The assessment & hardening of the private network will begin with the port locks and continue with post moves and equipment surplus as noted in the AAR. Our ultimate goal is to collectively remove all unnecessary services/hardware from the network and further secure and improve the remaining/new systems. I've asked Chris Dehner to take point and, working with his embedded staff, develop a plan for these items.

As always, please let me know if you have any additional questions or if I can assist further in any way,

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

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Merle King" <mking@kennesaw.edu>
Sent: Thursday, April 27, 2017 10:39:08 AM
Subject: FW: Private Network Hardware Assessment

Stephen,

Here is the email Steven Dean sent Chris Dehner yesterday.

Michael Barnes
Director
Center for Election Systems
Kennesaw State University

3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Steven Dean [mailto:sdean29@kennesaw.edu]
Sent: Wednesday, April 26, 2017 3:18 PM
To: Christopher M. Dehner <cmd9090@kennesaw.edu>
Cc: Merle S. King <mking@kennesaw.edu>; Michael Barnes <mbarne28@kennesaw.edu>; Jason Figueroa <jfigue12@kennesaw.edu>
Subject: Private Network Hardware Assessment

Chris, we recently receive a draft of the Incident report and I would like to go through the hardware section to get a plan outlined for addressing the recommendations. The document states the following:

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 – Electors list creation box
   Recommendation: Continue as ISO/CES managed
6. EPIC Files – Dell 1900 – Age 6+ years – Electors list creation box backups
   Recommendation: Surplus
7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS
   Recommendation: Surplus
8. elections.kennesaw.edu <http://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

We had submitted for approval to UITS the purchase of two new UPS units prior to the incident. Should we continue and order these as previously

planned?

Will new hardware (and other equipment) be ordered by ISO under ISO budget, ordered by ISO under CES budget, or ordered by CES? Who will decide what hardware is purchased?

How should we proceed with replacing the Switches and who will install and manage them?

When will the assessment of the private network software commence and what department will handle the migrations and updates? How will this project factor into their schedule?

We would like to get moving on this list as soon as possible. Please let me know what I can do as the next step. Thanks.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

Michael Barnes

From: Stephen Craig Gay
Sent: Monday, March 20, 2017 8:54 AM
To: Christopher Michael Dehner
Cc: Steven Jay Dean; Michael L. Barnes; James Christopher Gaddis
Subject: Re: Request for data retrieval

Chris,

This server is physically secured in ISO Evidence Storage. Please coordinate with Chris Gaddis and Steven Dean on the Data Recovery this morning.

Stephen

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>, "Lectra Lawhorne" <llawhorn@kennesaw.edu>
Sent: Friday, March 17, 2017 9:10:57 AM
Subject: RE: Request for data retrieval

Stephen,

Thank you. Steven and Jason will be available first thing Monday to assist.

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012
-----Original Message-----
From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Friday, March 17, 2017 9:09 AM
To: Michael Barnes <mbarne28@kennesaw.edu>
Cc: Steven Dean <sdean29@kennesaw.edu>; Merle King <mking@kennesaw.edu>; Lectra Lawhorne <llawhorn@kennesaw.edu>
Subject: Re: Request for data retrieval

Michael,

I have contacted the Federal investigators and they have agreed to return the server. I will be meeting with them late this afternoon to receive it and then secure it within ISO Secure Storage. I have asked the team to make this a top priority and to work with Steven and Jason on the request data retrieval 1st thing on Monday.

Please let me know if you have any questions or if I can assist further in any way, Stephen

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, March 15, 2017 1:41:25 PM
Subject: Request for data retrieval

Stephen,

As discussed earlier today, we would like to retrieve certain records from elections.kennesaw.edu that support our daily office activities, items such as inventory records, workflow databases used during our ballot building efforts, and operation manuals. These data are located in the cesuser user directory at /home/cesuser. We would like to retrieve the entire cesuser directory, if possible.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

Michael Barnes

From: Steven Dean <stevendean@kennesaw.edu>
Sent: Wednesday, March 29, 2017 1:43 PM
To: James Christopher Gaddis
Cc: Christopher Michael Dehner
Subject: Re: Unknown files on elections.kennesaw.edu

Importance: High

Chris, here are the data contained in each of the file types you have listed:

>mpearso9/ExpressPoll/L&AFiles/PollData.db3

This type of file may contain a subset of the list of voters and any associated voter information for a given election. The file is used for testing purposes by counties before using an ExpressPoll during an election. The directory listed here indicates that this file was for CES testing purposes and may not contain PII.

>ExpressPoll%20L%26A/PollData.db3.php
>Test%20Staff/ExpressPoll/ABSFile/PollData.db3.php
>County%20User/ExpressPoll/ABSFile/PollData.db3.php

These files enable download of associated "PollData.db3" files by every browser. Note: these are PHP files that only link to other files and do not contain any election data.

>/sites/default/files/vendors/ESandS/Primary%202010.zip

Without analyzing this file, I cannot say for certain what is in it. Previous emails from ISO have indicated that inspection of this file showed it to contain voter information from the time the file was created in 2010. May contain PII.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Mar 29, 2017, at 1:15 PM, Chris Gaddis <jgaddis6@KENNESAW.EDU> wrote:
>
> Steven,
>
> Can you please help me understand what data was contain in the files listed below.
>
> Was this County data?
> Full state data?
> Other Pii?
> Something else?

Also can you please respond ASAP on this.

Unique file names

ExpressPoll%20L%26A/PollData.db3.php
mpearso9/ExpressPoll/L&AFiles/PollData.db3
Test%20Staff/ExpressPoll/ABSFile/PollData.db3.php
County%20User/ExpressPoll/ABSFile/PollData.db3.php
/sites/default/files/vendors/ESandS/Primary%202010.zip

Thanks so much!

-Chris

Michael Barnes

From: Steven Dean <stevendean@kennesaw.edu>
Sent: Wednesday, March 01, 2017 11:49 PM
To: Merle Steven King
Cc: Michael L. Barnes
Subject: Re: Vulnerability on the elections.kennesaw.edu website

Acknowledging that I've seen this. See you tomorrow.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Mar 1, 2017, at 11:44 PM, Merle S. King <mking@kennesaw.edu> wrote:

> FYI.
>
> Sent from my iPad
>
> Begin forwarded message:
>
> **From:** "Stephen C. Gay" <sgay@kennesaw.edu>
> **Date:** March 1, 2017 at 11:10:16 PM EST
> **To:** Merle King <mking@kennesaw.edu>, Steven Dean <sdean29@kennesaw.edu>
> **Cc:** Lectra Lawhorne <llawhorn@kennesaw.edu>, "William C. Moore" <wmoore36@kennesaw.edu>
> **Subject: Fwd: Vulnerability on the elections.kennesaw.edu website**
>
> 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

73656d70657220706172617261747573

Bill, we updated the production server last night and I initiated a scan this morning. It looks really good to me, I'll just need your guidance on what issues we should address immediately. Thank you again for you and your department's work on the security on campus. This has been a huge help to us.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Oct 12, 2016, at 5:53 PM, Steven Dean <stevendean@kennesaw.edu> wrote:

Bill, thank you! This is great news. The unicoi server doesn't have an ssl cert so the plain text log-ins over http will be corrected when we role the updates into the production server.

Samba shouldn't be running on these servers so that is also easily remedied.

Elections.kennesaw hasn't been updated yet, so that's why you're seeing all of the same vulnerabilities. Now that we've confirmed the updates fix most if not all of the vulnerabilities, we will work after hours in the coming days to transition elections.kennesaw to the latest versions of Debian and PHP, as is currently the case on unicoi.

Thank you for all your help with this, we will let you know when we are ready for the next round of scans.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Wed, Oct 12, 2016 at 2:25 PM -0400, "William C. Moore" <wcmoore@kennesaw.edu> wrote:

Steven,

We have scanned both elections and Unicoi servers with basic level scans. The scan of the Unicoi server identified one critical vulnerability but we also noticed two pages that allowed plaintext logins

(http://unicoi.kennesaw.edu/?q=user/login and the samba-swat login http://unicoi.kennesaw.edu:901/) . I am sure that you are aware that these are opportunities for malicious users to gather account credentials. Therefore, all website logins should be passed through an SSL tunnel such as using https for authentication.

The critical vulnerability discovered on the Unicoi server is for "Invalid CIFS Logins Permitted" which is most likely related to the Samba Configuration file smb.conf (https://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html).

The server elections.kennesaw.edu however is still showing that an outdated version of PHP is running and may be the reason 40+ critical vulnerabilities are being identified as related to PHP.

Can you tell us what version of PHP is running and when we may be allowed to run a more through scan?

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 Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

From: Steven Dean [mailto:stevendean@kennesaw.edu]
Sent: Thursday, October 06, 2016 11:58
To: William C. Moore <wcmoore@kennesaw.edu>
Cc: Michael Barnes <mbarne28@kennesaw.edu>; Jason Figueroa <jfigue12@kennesaw.edu>; Chris Gaddis <jgaddis6@kennesaw.edu>; Merle S. King <mking@kennesaw.edu>; Stephen C. Gay <sgay@kennesaw.edu>
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Bill, we have the backup site up and running (thanks to G.J.!) on the new version of Debian with all packages updated. Can we have unicoi.kennesaw.edu added to NeXpose for scanning?

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Oct 4, 2016, at 4:41 PM, Steven Dean <stevendean@kennesaw.edu> wrote:

Bill, thank you for following up. So far we haven't heard from anyone who can help us reconfigure apache and have thus far been unable to get it working. I sent our apache server logs to Matt as requested. Has any information about our configuration come from them?

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Oct 4, 2016, at 4:37 PM, William C. Moore <wcmoore@kennesaw.edu> wrote:

Steven,

I and my team are taking the ISO lead on working with your team to help resolve any security issues with the server elections.kennesaw.edu. This is the last communication that I was copied on so can you

please provide me an update on where we stand on the server, PHP and Apache configurations? Where can we help and provide the greatest level of security support?

Thanks,

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 Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

From: Steven Dean [mailto:stevendean@kennesaw.edu]
Sent: Thursday, September 15, 2016 12:37
To: Matthew Sims <msims24@kennesaw.edu>
Cc: Michael Barnes <mbarne28@kennesaw.edu>; William C. Moore <wcmoore@kennesaw.edu>; Tyler Hayden <thayden2@kennesaw.edu>; Jason Figueroa <jfigue12@kennesaw.edu>; Chris Gaddis <jgaddis6@kennesaw.edu>; Merle S. King <mking@kennesaw.edu>
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Matt, we've the backup server updated to Debian Jessie, but with the changes to apache between versions, we've discovered we're a little out of our depth in trying to reconfigure apache to work with our website. Can you put us in touch with someone who may be able to help us get the website back up

on the backup server? We're probably up to date with security on the backup server, but it's all for naught if the website doesn't work ;-)

Thank you!

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Sep 12, 2016, at 11:55 AM, Matthew Sims <msims24@kennesaw.edu> wrote:

Steven,

I'm glad that the backup server is up and running. Thank you for the updates, and I hope your roll to production goes smoothly after testing.

From: "Steven Dean" <stevendean@kennesaw.edu>
To: "Matthew Sims" <msims24@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "William C. Moore" <wcmoore@kennesaw.edu>, "Tyler Hayden" <thayden2@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "Chris Gaddis" <jgaddis6@kennesaw.edu>, "Merle S. King" <mking@kennesaw.edu>
Sent: Friday, September 9, 2016 3:54:40 PM
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Good afternoon, Matt. We have our backup server up and running and just need to do a little testing before performing the updates. Once we confirm the distro update works on the backup server, we will roll the updates onto the production server and have you begin scans. This will give the most accurate scan results and tells us what we actually need help with security-wise. Thanks for your patience and the offer of help. I'll send you another update early next week. Have a great weekend.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road

Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Sep 7, 2016, at 5:03 PM, Matthew Sims <msims24@kennesaw.edu> wrote:

Steven,

Thank you for the updates and transparency. We look forward to hearing back from you.

Have a good afternoon.

From: "Steven Dean" <stevendean@kennesaw.edu>
To: "Matthew Sims" <msims24@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "William C. Moore" <wcmoore@kennesaw.edu>, "Tyler Hayden" <thayden2@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "Chris Gaddis" <jgaddis6@kennesaw.edu>
Sent: Wednesday, September 7, 2016 4:43:28 PM
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Matt, we're still working on getting a fully working clone on another server to perform the updates on. Once we have that working we'll roll the updates onto the production server. Then you can begin a new round of testing through NeXpose. Unfortunately, getting the updates completed with proper backups and testing has been slow going because of the election build, but that is all but passed and we are now working to get the server updated.

We will send you an update tomorrow on our progress and we should have a day for you to begin the new round of testing.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Sep 7, 2016, at 3:29 PM, Matthew Sims <msims24@kennesaw.edu> wrote:

Hi Michael,

I wanted to touch base with you and see what our game plan will be moving forward. Are we still in the stages of upgrading the OS and PHP version or has that already happened? In terms of scanning at the application level, I am trying to iron out a timeline and determine when this can be done using more aggressive scanning similar to Nexpose, but if you are going to be upgrading the OS and PHP version, then I may need to wait and coordinate a later time.

Thanks for your time and please let me know what you think.

From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "William C. Moore" <wcmoore@kennesaw.edu>
Cc: "Steven Dean" <stevendean@kennesaw.edu>, "Tyler Hayden" <thayden2@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "Matthew Sims" <msims24@kennesaw.edu>, "Chris Gaddis" <jgaddis6@kennesaw.edu>
Sent: Friday, September 2, 2016 5:59:17 PM
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Bill,

Thank you. I will be back in touch on Tuesday to discuss when we would like for these scans to begin.

Sincerely,

Michael Barnes

Director

Center for Election Systems

3205 Campus Loop Road

Kennesaw State University

Kennesaw, GA 30144

ph: 470-578-6900

On Sep 2, 2016, at 5:55 PM, William C. Moore <wcmoore@kennesaw.edu> wrote:

Michael,

The directive to begin more agressive scanning came from Stephen Gay to help ensure that the server was not posing a risk to the Center of Elections missions and objectives.

The probability of damaging your website should be low. We do not wish to take any action that would actually damage any of your data or website(s). Typically a large portion of emails are sent by the

scanning engines auto completing website forms tha are not properly protected. These are usually more of an annoyance than any real damage.

The server does however have a number of critical and severe vulnerabilities some of which are reported to be exploitable. The majority of these are centered around PHP but others are OS related. These may be problematic but we would much rather test under controlled environments instead of the system becoming exploited during a time when your services are under high scrutiny and in great demand by polling stations around the state.

Since we would control the assessment tools the Information Security Office would be able to stop any assessments we (the ISO) are performing as soon as you noticed a degradation in services via a phone call to our team. Of course, I suspect that you have current backups of your website and data in case any other persons are performing malicious attacks against the Center of Elections. We do not of course anticipate you needing these backups for our assessments but you should still keep them and the restoration process up-to-date as a best practice. The Information Security Office does not want to impede the Center's objectives at all. We want to help mitigate any risks that the Center is facing such as the risks that Mr. Lamb from the Bastille Threat Research Team discovered and reported. There are a number of documents found from the Center of Elections website that have been cached by various search engines. These are not threats that we can now prevent; however, we can offer suggestions on how to request those cached documents be removed from the various search engine providers.

I hope that this addresses some of your concerns and since this has to be a two way partnership in our assessment we encourage you to ask questions along the way.

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 Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "William C. Moore" <wcmoore@kennesaw.edu>, "Steven Dean" <stevendean@kennesaw.edu>
Cc: "Tyler Hayden" <thayden2@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "Matthew Sims" <msims24@kennesaw.edu>, "Chris Gaddis" <jgaddis6@kennesaw.edu>
Sent: Wednesday, August 31, 2016 3:15:46 PM
Subject: RE: [IMPORTANT] concerning the security of elections.kennesaw.edu

Bill,

Before we give go ahead on potential scan periods I have a couple of follow up questions:

1. The directive to begin more aggressive scanning has come from who and for what reason?

2. How high a probability is there of issues being created that could damage the functionality of our website?

We are currently in the busiest time of the year for use of our website by our county clients. The last thing we can afford to have happen is for our website to become unavailable or usable. If the action of conducting these scans were to disable our website, what remedy would be available so the services we provide to the election community in Georgia would not be damaged?

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: William C. Moore [mailto:wcmoore@kennesaw.edu]
Sent: Wednesday, August 31, 2016 2:47 PM
To: 'Steven Dean' <stevendean@kennesaw.edu>
Cc: 'Tyler Hayden' <thayden2@kennesaw.edu>; 'Michael Barnes' <mbarne28@kennesaw.edu>; 'Jason Figueroa' <jfigue12@kennesaw.edu>; 'Matthew Sims' <msims24@kennesaw.edu>; Chris Gaddis <jgaddis6@kennesaw.edu>
Subject: RE: [IMPORTANT] concerning the security of elections.kennesaw.edu

Steven,

The recent scans have been "Safe Scans w/o Spidering". I have been asked though to begin more aggressive scanning. Since these types of scans have the potential of creating issues such as completing and submitting forms

(creating email messages) interfering with services and/or stopping services which we try to avoid. Since these assessments have the potential of creating issues we need to schedule these types of assessments. Please understand that we do not perform any testing that cannot already be performed by any user on the campus network. We also do not purposefully perform any DOS or DDOS attempts since the network perimeter firewalls provide some level of protection against DDOS attempts.

When is the earliest we can schedule more aggressive scanning of the server?

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 Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu>

From: Steven Dean [mailto:stevendean@kennesaw.edu]
Sent: Wednesday, August 31, 2016 10:38
To: William C. Moore <wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu> >
Cc: Tyler Hayden <thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu> >;
Michael Barnes <mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu> >;
Jason Figueroa <jfigue12@kennesaw.edu<mailto:jfigue12@kennesaw.edu> >;
Matthew Sims <msims24@kennesaw.edu<mailto:msims24@kennesaw.edu> >
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Thanks Bill. I see the list appears to be the same as from the first scan. Jason and I are working on a plan to upgrade to the latest version of Debian which will also allow us to update to the latest version of PHP, where it seems most of the vulnerabilities are. Let me know if there is anything in the scan we should be concerned about that the Debian update may not fix. Thanks for all the help, we really appreciate your time. It has been immensely beneficial.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Aug 31, 2016, at 10:34 AM, William C. Moore <wcmoore@kennesaw.edu <mailto:wcmoore@kennesaw.edu> > wrote:

Steven

The authenticated scan completed last night and I will share the results as soon as my current meeting completes.

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 Pl

Kennesaw, GA 30144

Tel: 470-578-6620

Fax: 678-915-4940

wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu>

On Aug 31, 2016, at 10:00, Steven Dean <stevendean@kennesaw.edu <mailto:stevendean@kennesaw.edu> > wrote:

Sounds good to us. Thanks Tyler.

What is the status of the authenticated scan? I couldn't find where it had been run and when I went to run a scan, the available options made it difficult to choose while not really understanding them.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Wed, Aug 31, 2016 at 9:56 AM -0400, "Tyler Hayden" <thayden2@kennesaw.edu <mailto:thayden2@kennesaw.edu> > wrote:

Hi Steven,

In addition to the NeXpose scan, we'd also like to scan with IBM AppScan. AppScan will focus more specifically on the Drupal application rather than an overarching system scan with NeXpose. Matt Sims will reach out to you to configure and schedule the AppScan assessment.

Regards,

Tyler Hayden
IT Security Professional III
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503

Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9051
thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu>

----- Original Message -----
From: "William C. Moore" <wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu>

To: "Steven Dean" <sdean29@kennesaw.edu<mailto:sdean29@kennesaw.edu> >
Cc: "Tyler Hayden" <thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu> >,
"Michael Barnes" <mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu> >,
"Jason Figueroa" <jfigue12@kennesaw.edu<mailto:jfigue12@kennesaw.edu> >,
"Matthew Sims" <msims24@kennesaw.edu<mailto:msims24@kennesaw.edu> >
Sent: Tuesday, August 30, 2016 2:03:57 PM
Subject: RE: [IMPORTANT] concerning the security of elections.kennesaw.edu
<http://elections.kennesaw.edu/>

Yes, this will be a local Linux account. It is preferable that the account be provided sudo privileges only. I strongly recommend that you limit the account to only be allowed to log in locally for your testing purposes and from the IP addresses 130.218.100.80 and 10.97.52.25 (the two current Nexpose scanning engines).

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 Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu>

From: Steven Dean [mailto:sdean29@kennesaw.edu]
Sent: Tuesday, August 30, 2016 12:21
To: William C. Moore <wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu> >
Cc: Tyler Hayden <thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu> >;
Michael Barnes
<mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu> >; Jason Figueroa
<jfigue12@kennesaw.edu<mailto:jfigue12@kennesaw.edu> >; Matthew
Sims <msims24@kennesaw.edu<mailto:msims24@kennesaw.edu> >
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu
<http://elections.kennesaw.edu/>

Just to clarify, are the required credentials a linux account for the server itself? Also, could you define "privileged account"? Does it need to be an admin or just have sudo ability?

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Aug 30, 2016, at 11:59 AM, William C. Moore <wcmoore@kennesaw.edu
<mailto:wcmoore@kennesaw.edu>
<mailto:wcmoore@kennesaw.edu> > wrote:

Steven,

Please log back in to Nexpose and use the following steps to add an account for patching and vulnerability verification.

Select Home then scroll though Sites until you find the site "Elections-Server".

Select the Edit icon (pencil) for the Elections-Server site.

Select the Authentication tab at the top of the page.

Click the "Elections-Server-Account" link under Scan Credentials.

You should now be in the Edit Credential page. From this page select

"Account" on the left hand side of the page.

This page already has the Service as Secure Shell (SSH) selected. You should enter the User Name and enter the appropriate password in both the Password field and Confirm Password field.

After you have entered and confirmed the account credentials please click the "Test Credentials" link beside the question mark near the bottom of the page to verify the account and credentials work.

After successfully testing the credentials click the Save button at the bottom of the page then click the Save button at the top right hand side of the page.

Please let us know when you have added, tested and saved the authentication information and we will test the site again for vulnerabilities.

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 Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
<mailto:wcmoore@kennesaw.edu> wcmoore@kennesaw.edu
<mailto:wcmoore@kennesaw.edu>

From: Steven Dean [mailto:sdean29@kennesaw.edu]
Sent: Monday, August 29, 2016 16:46
To: Tyler Hayden <thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu>
<mailto:thayden2@kennesaw.edu> >

Cc: Michael Barnes <mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu>
<mailto:mbarne28@kennesaw.edu> >;
Jason Figueroa <jfigue12@kennesaw.edu<mailto:jfigue12@kennesaw.edu>
<mailto:jfigue12@kennesaw.edu> >;
Matthew Sims <msims24@kennesaw.edu<mailto:msims24@kennesaw.edu>
<mailto:msims24@kennesaw.edu> >; William
C. Moore <wmoore36@kennesaw.edu<mailto:wmoore36@kennesaw.edu>
<mailto:wmoore36@kennesaw.edu> >
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu
<http://elections.kennesaw.edu/>
<http://elections.kennesaw.edu<http://elections.kennesaw.edu%3e> >;

Thanks Tyler. I've logged into NeXpose so we're ready to have our server added. Server info:

Hostname: <http://elections.kennesaw.edu/
<http://elections.kennesaw.edu/%3E> >; elections.kennesaw.edu
<http://elections.kennesaw.edu/>

IP: 130.218.251.50

OS: Debian Wheezy v7.11

Hosted Application: Drupal 7.5

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Aug 29, 2016, at 4:22 PM, Tyler Hayden < <mailto:thayden2@kennesaw.edu>
thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu> > wrote:

Hi Steven,

Thanks for reaching out. We can definitely assist in assessing the security and of your site. For starters, we can arrange for a security and vulnerability assessment scan on your systems via NeXpose to get some better insight.

We can scan both authenticated or unauthenticated. Authenticated scans will

produce more accurate results, but also require credentials for a privileged account. We can configure it to allow you to log in to NeXpose to provide these credentials, if you do not want to provide them to us directly. We'll just need information on the systems you'd want assessed. (Host names, OS, IP address, hosted applications, etc.)

While I am not all too familiar with Drupal, I do know that there are several modules available for restricting content in Drupal, such as the Secure Site module which is available here:

<https://www.drupal.org/project/securesite
<https://www.drupal.org/project/securesite%3E> >;
https://www.drupal.org/project/securesite

This is just one of the available modules, so if this does not suit your needs there are others available. I would also review Drupal's documentation on secure configuration available here:

<https://www.drupal.org/security/secure-configuration
<https://www.drupal.org/security/secure-configuration%3E> >;
https://www.drupal.org/security/secure-configuration

to ensure that your site is following their best practices.

Without doing some research of my own, I am not certain on how to go about restricting file access using the htaccess files. Typically you would include a directive to only allow authenticated users to access the file, however, I am not certain of how Drupal handles it's authentication or if it shares it with the Apache web server. This is something we can look into and let you know what we find.

Regards,

Tyler Hayden
IT Security Professional III
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9051
<mailto:thayden2@kennesaw.edu> thayden2@kennesaw.edu
<mailto:thayden2@kennesaw.edu>

----- Original Message -----
From: "Steven Dean" < <mailto:sdean29@kennesaw.edu> sdean29@kennesaw.edu
<mailto:sdean29@kennesaw.edu> >
To: "Tyler Ray Hayden" < <mailto:thayden2@kennesaw.edu>
thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu> >

Cc: "Michael Barnes" < <mailto:mbarne28@kennesaw.edu>
mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu> >, "Merle S. King" <
<mailto:mking@kennesaw.edu>
mking@kennesaw.edu<mailto:mking@kennesaw.edu> >, "Jason Figueroa" <
<mailto:jfigue12@kennesaw.edu>
jfigue12@kennesaw.edu<mailto:jfigue12@kennesaw.edu> >
Sent: Monday, August 29, 2016 2:39:41 PM
Subject: Re: [IMPORTANT] concerning the security of
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
elections.kennesaw.edu<http://elections.kennesaw.edu/>

Good afternoon, Tyler. I wanted to reach out for some assistance with our website as suggested in Stephen's email below.

For some background information, Jason and I have taken responsibility for the website here at Center for Election Systems. This site was build on Drupal before either of us were employed here and we have spent the last several years simply maintaining it in the order it had been working previously. Obviously this has become untenable in the current atmosphere, and Jason and I must learn more to get the security of the website under control. In this regard we appreciate any help you can offer on security best practices and specific security implementations that will allow us to secure the site.

This morning we implemented a patch to disallow file tree access by anonymous users and we updated our Drupal installation to the current version of Drupal 7. Unfortunately, until today, it seems the file tree had been available to anonymous users. We have denied access by changing the "AllowOverride None" in the apache virtualhost configuration for /var/www/ to "AllowOverride All" so that the .htaccess file parameters will disallow anonymous user access outside Drupal.

While we have denied access to the file tree, we are currently we are having trouble patching the ability for anonymous users to access individual files directly without also disallowing Drupal user access to those files. We have tried adding a <files> tag section tot he apache2.conf to deny access to pdf files, but this breaks Drupal user access as well. I'm sure there is some way to do this in the .htaccess file, but we have so far been unable to find the method.

Please let Jason and I know if you have any insights that will help accomplish this goal, as well as get a local firewall set up to allow us to monitor access through logs.

Thank you,

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Aug 29, 2016, at 11:31 AM, Stephen C. Gay < <mailto:sgay@kennesaw.edu> sgay@kennesaw.edu<mailto:sgay@kennesaw.edu> > wrote:

Michael,

Thanks for reaching out and we stand on ready to help. The source email domain, <http://bastille.net/<http://bastille.net/%3E> >; bastille.net <http://bastille.net/> < <http://bastille.net/<http://bastille.net/%3E> >; http://bastille.net/ <http://bastille.net/%3E> >;, has a valid domain registration through GoDaddy and
located in Atlanta:

Registry Registrant ID:
Registrant Name: Michael Engle
Registrant Organization: Bastille Networks
Registrant Street: 1000 Marietta St NW
Registrant Street: Suite 112
Registrant City: Atlanta
Registrant State/Province: GA
Registrant Postal Code: 30318
Registrant Country: US
Registrant Phone: +1.7328200096
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: <mailto:domains@bastillenetworks.com> domains@bastillenetworks.com<mailto:domains@bastillenetworks.com> < <mailto:domains@bastillenetworks.com> mailto:domains@bastillenetworks.com>

We don't put internal domain blocks in place unless we detect a spike in phishing or vulnerability scanning from that domain which, at this point, isn't the case for <http://bastille.net/<http://bastille.net/%3E> >; bastille.net <http://bastille.net/> < <http://bastille.net/ <http://bastille.net/%3E> >; http://bastille.net/ <http://bastille.net/%3E> >;. It's very likely that the tester utilized Google searches on the <http://elections.kennesaw.edu/ <http://elections.kennesaw.edu/%3E> >; elections.kennesaw.edu<http://elections.kennesaw.edu/> < <http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >; http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >; domain which included file extensions, along
with HTML Headers which include the service versions.

Here the the Google search string which reveals the document he references
".pdf site:elections.kennesaw.edu"
Reporting precincts with cards -

<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L
<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L&A/Reporting%20Precincts%20with%20Cards.pdf%3E>
&A/Reporting%20Precincts%20with%20Cards.pdf>;
https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L
<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L&A/Reporting%20Precincts%20with%20Cards.pdf%3C>
&A/Reporting%20Precincts%20with%20Cards.pdf<;
<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L
<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L&A/Reporting%20Precincts%20with%20Cards.pdf%3E>
&A/Reporting%20Precincts%20with%20Cards.pdf>;
https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L
<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L&A/Reporting%20Precincts%20with%20Cards.pdf%3E>
&A/Reporting%20Precincts%20with%20Cards.pdf>;

And here is the header response for
<https://elections.kennesaw.edu/?q=user/login
<https://elections.kennesaw.edu/?q=user/login%3E> >;
https://elections.kennesaw.edu/?q=user/login
<https://elections.kennesaw.edu/?q=user/login%3C> <;
<https://elections.kennesaw.edu/?q=user/login
<https://elections.kennesaw.edu/?q=user/login%3E> >;
https://elections.kennesaw.edu/?q=user/login
<https://elections.kennesaw.edu/?q=user/login%3E> >; that gives away the use
of
Drupal
<https://elections.kennesaw.edu/misc/drupal.js?ococft
<https://elections.kennesaw.edu/misc/drupal.js?ococft%3E> >;
https://elections.kennesaw.edu/misc/drupal.js?ococft <
<https://elections.kennesaw.edu/misc/drupal.js?ococft
<https://elections.kennesaw.edu/misc/drupal.js?ococft%3E> >;
https://elections.kennesaw.edu/misc/drupal.js?ococft
<https://elections.kennesaw.edu/misc/drupal.js?ococft%3E> >;

It is reasonable to assume that these types of unsolicited requests are going to increase leading up to the general election in November and we stand on ready to offer application security analysis and recommendations. In turn, I would highly recommend the use of an server based firewall/IDS to track this activity (specifically brute force attempts on the login page) and ensure that all access are logged.

I am cc'ing 2 members of my team, Mr. Tyler Haden and Mr. Bill Moore, to advise on operating system/application vulnerabilities and provide advice on mitigating strategies. Tyler will act as your point of contact and if I can assist in any way please let me know.

In service,

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
<mailto:sgay@kennesaw.edu> sgay@kennesaw.edu<mailto:sgay@kennesaw.edu> <
<mailto:sgay@kennesaw.edu>
mailto:sgay@kennesaw.edu>

----- Original Message -----
From: "Michael Barnes" < <mailto:mbarne28@kennesaw.edu>
mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu> <
<mailto:mbarne28@kennesaw.edu>
mailto:mbarne28@kennesaw.edu>>
To: "Stephen C Gay" < <mailto:sgay@kennesaw.edu> sgay@kennesaw.edu
<mailto:sgay@kennesaw.edu> <
<mailto:sgay@kennesaw.edu> mailto:sgay@kennesaw.edu>>
Cc: "Merle King" < <mailto:mking@kennesaw.edu> mking@kennesaw.edu
<mailto:mking@kennesaw.edu> <
<mailto:mking@kennesaw.edu> mailto:mking@kennesaw.edu>>, "Steven Dean" <
<mailto:sdean29@kennesaw.edu> sdean29@kennesaw.edu
<mailto:sdean29@kennesaw.edu> <
<mailto:sdean29@kennesaw.edu> mailto:sdean29@kennesaw.edu>>, "Jason
Figueroa" < <mailto:jfigue12@kennesaw.edu> jfigue12@kennesaw.edu
<mailto:jfigue12@kennesaw.edu> <
<mailto:jfigue12@kennesaw.edu> mailto:jfigue12@kennesaw.edu>>
Sent: Monday, August 29, 2016 9:24:30 AM
Subject: FW: [IMPORTANT] concerning the security of
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
elections.kennesaw.edu<http://elections.kennesaw.edu/> <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;

Stephen,

We received an unsolicited email over the weekend from a Logan Lamb. The content of the email has engaged our staff and we are looking into these claims regarding the security of our website. Would you please add this individual and the organization he claims to be affiliated with to the list of IP addresses most recently black listed? Also, our IT staff, Steven Dean and Jason Figueroa will be reaching out to you and your staff to see what assistance your group can provide us in pinging our site to verify that we are addressing security issues within our site.

Thank you in advance,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Merle S. King [<mailto:mking@kennesaw.edu> mailto:mking@kennesaw.edu]
Sent: Sunday, August 28, 2016 3:56 PM
To: Steven Dean < <mailto:sdean29@kennesaw.edu> sdean29@kennesaw.edu
<mailto:sdean29@kennesaw.edu> >; Jason
Figueroa
< <mailto:jfigue12@kennesaw.edu> jfigue12@kennesaw.edu
<mailto:jfigue12@kennesaw.edu> >
Cc: Michael Barnes < <mailto:mbarne28@kennesaw.edu> mbarne28@kennesaw.edu
<mailto:mbarne28@kennesaw.edu> >
Subject: Fwd: [IMPORTANT] concerning the security of
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
elections.kennesaw.edu<http://elections.kennesaw.edu/>

Steven and Jason - Please review this email and advise. Sooner is better
than later.

Thanks,

MSK

From: "Logan Lamb" < <mailto:logan@bastille.net> logan@bastille.net
<mailto:logan@bastille.net> <
<mailto:logan@bastille.net> mailto:logan@bastille.net> <
<mailto:logan@bastille.net> mailto:logan@bastille.net<
<mailto:logan@bastille.net> mailto:logan@bastille.net>> >
To: "Merle King" < <mailto:mking@kennesaw.edu> mking@kennesaw.edu
<mailto:mking@kennesaw.edu> <
<mailto:mking@kennesaw.edu> mailto:mking@kennesaw.edu> <
<mailto:mking@kennesaw.edu> mailto:mking@kennesaw.edu<
<mailto:mking@kennesaw.edu> mailto:mking@kennesaw.edu>> >

Cc: <mailto:research@bastille.net> research@bastille.net
<mailto:research@bastille.net> <
<mailto:research@bastille.net> mailto:research@bastille.net> <
<mailto:research@bastille.net> mailto:research@bastille.net<
<mailto:research@bastille.net> mailto:research@bastille.net>>
Sent: Sunday, August 28, 2016 3:47:50 PM
Subject: [IMPORTANT] concerning the security of
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
elections.kennesaw.edu<http://elections.kennesaw.edu/> <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;

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/
<https://www.bastille.net/%3E> >;
https://www.bastille.net/ < <https://www.bastille.net/
<https://www.bastille.net/%3E> >;
https://www.bastille.net/<https://www.bastille.net/%3E> >;. 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

<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
elections.kennesaw.edu<http://elections.kennesaw.edu/> <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >; <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu<http://elections.kennesaw.edu%3c> <;
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E%3E> >>; .

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 < <http://elections.kennesaw.edu/
<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu<http://elections.kennesaw.edu/> <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E%3E> >>;
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 < <http://elections.kennesaw.edu/
<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu<http://elections.kennesaw.edu/> <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E%3E> >>;
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/project/drupalgeddon%3E> >;
https://www.drupal.org/project/drupalgeddon<
<https://www.drupal.org/project/drupalgeddon
<https://www.drupal.org/project/drupalgeddon%3E> >;
https://www.drupal.org/project/drupalgeddon
<https://www.drupal.org/project/drupalgeddon%3E> >;

<https://www.drupal.org/SA-CORE-2014-005
<https://www.drupal.org/SA-CORE-2014-005%3E> >;
https://www.drupal.org/SA-CORE-2014-005<
<https://www.drupal.org/SA-CORE-2014-005
<https://www.drupal.org/SA-CORE-2014-005%3E> >;
https://www.drupal.org/SA-CORE-2014-005
<https://www.drupal.org/SA-CORE-2014-005%3E> >;

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

--

Merle S. King

Executive Director

Center for Election Systems

Kennesaw State University

3205 Campus Loop Road

Kennesaw, Georgia 30144

Voice: 470-578-6900
Fax: 470-578-9012

--

Matt Sims
Information Security Specialist

Identity & Access Management
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
msims24@kennesaw.edu

--

Matt Sims
Information Security Specialist

Identity & Access Management
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
msims24@kennesaw.edu

--

Matt Sims
Information Security Specialist

Identity & Access Management
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503
Kennesaw, GA 30144

Phone: (470) 578-6620
msims24@kennesaw.edu

DECLARATION OF CARRI GIBBS LUSE

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

DONNA CURLING, et al.	)	
Plaintiff,	)	
vs.	)	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**
BRIAN P. KEMP, et al.	)	
Defendant.	)	

DECLARATION OF CARRI GIBBS LUSE

CARRI GIBBS LUSE hereby declares as follows:

1. I am have been a Georgia voter since at least 1992 and am currently registered to vote at 175 Sampson Street NE, Atlanta, Georgia 30312, in Fulton County. I have been registered to vote at this address since November 2013.
2. On May 1, 2018 I voted in early voting at the Fulton County Elections Office at 140 Pryor Street, Atlanta in the May 22, 2018 primary.
3. I made a special trip to the central Elections Office to vote because I felt more confident of my early vote being counted at the central office than at a remote voting location. I took my mother to vote there at the same time.

4. I requested a Democratic Party ballot by completing the voter application certificate, specifying the Democratic Party ballot. I voted a Democratic Party electronic ballot on the touchscreen, and later proudly told friends about the candidates I selected on my ballot. I am very confident that I voted a Democratic Party ballot on the touchscreen machine that day.
5. On July 2, 2018 I voted in the July 24, 2018 runoff during early voting, this time choosing to vote in the Ponce de Leon Library early voting location.
6. When I checked in to vote that day and asked for a Democratic ballot, the pollworkers claimed that I had voted a Republican Party ballot in May, and could not vote a Democratic Party ballot in the runoff. I was in disbelief and continued to challenge the pollworkers, as I was confident that I voted a Democratic Party ballot in May.
7. I repeatedly asked what could be done to correct this error and vote a Democratic Party ballot, and the poll workers said that nothing could be done, and permitted me only to vote a Republican ballot or a non-partisan ballot, or not vote at all.
8. The pollworkers did not offer to let me vote a Democratic Party provisional ballot, despite my repeated request for a solution so that I

could vote for Democrats. I don't understand why I was not offered a provisional ballot which could have been counted after reviewing my May 1, 2018 voter application documenting the fact that I requested a Democratic ballot.

9. I am concerned that I was disenfranchised in this way, and concerned about the integrity of the electronic pollbooks that contain this error that caused my disenfranchisement. I am concerned that I might be further disenfranchised in the November election by other types of electronic election records errors.

10. I have read a number of recent reports of voter disenfranchisement, electronic pollbook errors, and voting machine errors, and I now have grave concerns about the integrity of the upcoming November election.

11. Because of my concerns about the integrity of the electronic election records in Georgia, I am researching the procedure and pros and cons of voting a paper mail-in ballot in November. It is my preference to have the flexibility of voting on Election Day in my home precinct, as I may want to wait until Election Day to obtain all last minute information about all campaigns, and not be required to vote several days before Election Day to assure that my mail ballot arrives in time

to be counted. If I have to make a choice between casting a secure verifiable ballot and the convenience of voting in my precinct on Election Day, I will choose to cast a mail-in paper ballot the week before the election.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, July 31, 2018.

Carri Gibbs Luse

DECLARATION OF MARILYN MARKS

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

DONNA CURLING, ET AL., **Plaintiffs** **, v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF MARILYN MARKS

MARILYN MARKS hereby declares as follows:

1. I am Executive Director of Coalition for Good Government, a Plaintiff in this action.

2. Attached as Exhibit 1 are true and correct copies of documents received by Coalition from Fulton County Board of Elections on June 7, 2017 at a hearing in the matter of Curling v Kemp (2017cv290630)

3. Attached as Exhibit 2 are true and correct copies of a sample of documents showing differences between the number of voters reported as voting at the polling place on Election Day and the number of ballots cast as reported on the polling place DRE machine results tapes. The documents were obtained from Fulton County Board of Elections as part of the agreed on DRE inventory information submission in this action.

4. Attached as Exhibit 3 are true and correct copies of documents appearing to show greater than 100% voter turnout. The documents are screenshots taken from

official reports from the Secretary of State's election results pages on website: http://sos.ga.gov/index.php/Elections/current_and_past_elections_results)

5. This is a link to a news report describing how electronic pollbook eliminated some voters' records with recent 4 digit zipcode suffix additions, forcing them to vote by provisional ballot: https://www.11alive.com/article/news/politics/voters-in-certain-metro-atlanta-counties-say-they-were-given-provisional-ballots-because-of-this/85-577127862.

6. Attached as Exhibit 4 is a screen shot from Secretary of State's election results pages on website: (http://sos.ga.gov/index.php/Elections/current_and_past_elections_results) from the November 8, 2016 election showing a DRE machine vote for a Congressional District 6 candidate from a precinct in Congressional District 5.

7. Attached as Exhibit 5 is a letter dated August 1, 2018 addressed to County Election Officials and Registrars from State Elections Division Director, Chris Harvey. I obtained this letter from Stephens County voter Packy McKibben via email who reported that he had obtained it as a public document at the August 2, 2018 Stephens County Board of Elections meeting.

In accordance with 28 U.S.C. § 1746, I pledge under penalty of perjury that the foregoing is true and correct.

Executed on this date, August 3, 2018.

Marilyn Marks

EXHIBIT 1

Ringer, Cheryl

From: Jones, Ralph
Sent: Thursday, April 20, 2017 1:08 PM
To: Brower, Dwight
Subject: FW: Elections Complaint from Brian W Blosser
Attachments: image2.jpeg

From: Harris, Axiver [mailto:aharris@sos.ga.gov]
Sent: Thursday, April 20, 2017 9:00 AM
To: Jones, Ralph
Cc: Marshall, Shamira
Subject: FW: Elections Complaint from Brian W Blosser

Ralph or Shamira,

When you get time today can you look into this and see if he should have been in US Congress District 6? Looks like he had an address change at DDS? Read email below.

From: Simmons, Jessica
Sent: Thursday, April 20, 2017 8:51 AM
To: Harris, Axiver <aharris@sos.ga.gov>
Subject: FW: Elections Complaint from Brian W Blosser

Can you please have Fulton look into this?

Thanks!

From: Brian Blosser [mailto:bblosser@krystalco.com]
Sent: Wednesday, April 19, 2017 7:07 PM
To: Simmons, Jessica <jsimmons@sos.ga.gov>
Cc: Brian Blosser (bblosser@aol.com) <bblosser@aol.com>
Subject: Fwd: Elections Complaint from Brian W Blosser

Ms Simmons your facts assumptions are incorrect. There appears to be a big issue in your data base. Please see the below voter registration card from 2015 that shows both my current address (which your team claimed I did not have) and the proper voting precinct for this special election. I would appreciate your team making the corrections so we have no further issues. I have lost every confidence in what I would call an impractical voting system in Georgia and many issues surrounding this special election. When I am being told that I cannot vote because of my affiliation (by more than one individual) and that they knew how I voted in the last election is very concerning. Please verify that this has/ will be resolved by the next election (again my proof is below). I look forward to hearing back from you regarding this egregious error.

Brian Blosser
678-699-4153

MARKS DECLARATION

From: "Simmons, Jessica" <jsimmons@sos.ga.gov>
Date: April 19, 2017 at 12:39:17 PM EDT
To: "bblosser@aol.com" <bblosser@aol.com>
Subject: RE: Elections Complaint from Brian W Blosser

Mr. Blosser,

Thank you for contacting the Secretary of State's Office. According to your voter registration, you are in Congressional District 11 and State Senate District 6. The Special Election yesterday in Fulton was for Congressional District 6 and State Senate District 32.

If you feel that you are in not in the proper district, please call the Fulton County Registrar's Office at 404-612-3816.

Please let me know if you have any questions.

Thanks,

Jessica

-----Original Message-----
From: ElectionsComplaintAlerts@sos.ga.gov
[mailto:ElectionsComplaintAlerts@sos.ga.gov]
Sent: Wednesday, April 19, 2017 8:52 AM
To: electionscomplaints <electionscomplaints@sos.ga.gov>
Subject: Elections Complaint from Brian W Blosser

Name: Brian W Blosser
Phone: (678) 699-4153
Address: 5996 Mitchell Road, Apt 15
City: Atlanta
State: GA
Zip Code: 30328
E-mail: bblosser@aol.com
Complaint Type: Turned Away at the Poll
Election Date:
County: Fulton
City: Atlanta

Description of Complaint: I was not allowed to vote due to my "affiliation". I asked how they know what my affiliation is. The reply was "by the way you voted in the last election". I have a valid voter registration card that was issued on 12/29/2015. Since the poll supervisor used the work "affiliation" the only reason I would have been turned away would be to surpress a republican/conservative vote. Please contact me for more details. Thank you.

This electronic transmission and any attached documents or other writings are confidential and are for the sole use of the intended recipient(s) identified above. This message may contain information that is privileged, confidential or otherwise protected from disclosure under applicable law. If you are the intended recipient, you are responsible for establishing appropriate safeguards to maintain data integrity and security. If the receiver of this information is not the intended recipient, or the employee, or agent responsible for delivering the information to the intended recipient, you are hereby notified that any use, reading, dissemination, distribution, copying or storage of this information is strictly prohibited. If you have received this information in error, please notify the sender and destroy the transmission, including all attachments from your system.

MARKS DECLARATION

VOTER REGISTRATION OFFICE
130 PEACHTREE STREET 2186
SW
ATLANTA GA 30303 - 3460
PHONE: 404-612-7020

FIRST CLASS MAIL
U.S. POSTAGE PAID
Atlanta, GA
PERMIT No: 2604

RETURN SERVICE REQUESTED

REG. DATE 03/27/2012
ISSUE DATE 12/29/2015
REG. No. 06966355

FULTON COUNTY PRECINCT CARD
SIGN CARD AND KEEP FOR YOUR RECORDS

PRECINCT NAME: SS31
POLLING PLACE: ABERNATHY ARTS CENTER
254 JOHNSON FERRY RD , SANDY SPRINGS GA 30328

CITY PRECINCT NAME: SS31
POLLING PLACE: ABERNATHY ARTS CENTER
254 JOHNSON FERRY RD , SANDY SPRINGS GA 30328

VOTING DISTRICTS:

006	006	052	004	3	3	03
CONG	SENATE	HOUSE	JUD	COMM	SCHOOL	CITYL

BRIAN W BLOSSER
5996 MITCHELL RD APT 15
ATLANTA GA 30328 - 4874

EXHIBIT 2

Exhibit 2.1
Fulton County Polling Place Recap Sheet Discrepancy
April 18, 2017 (Congressional District 6 Runoff)
Polling Place SS25

Note: The number of voters applying to vote at the polling place should reconcile to the number of ballots cast and number of votes reported with few, if any, reconciling items. The example recap sheet shows unreconciled differences. The number of ballots cast should not exceed the number of voters voting.

Information on Recap Sheet:

Reported ballots cast per DRE results tape=486

Reported number of voter certificates (voters voting)= 477

Reported election day votes for CD6 per official results= 479 (computed)
(http://results.enr.clarityelections.com/GA/Fulton/67378/Web02/#/)

ELECTION: (Check One)
- ☐ General
- ☐ Primary
- ☐ Runoff (if applicable)
- ☒ Special
- ☐ Presidential Preference Primary

USE BALL POINT PEN
Bear Down – You Are Making Three Copies

WHITE sheet to Secretary of State
YELLOW sheet to Superintendent
PINK sheet to Clerk of Superior Court or Municipal Clerk

DATE OF ELECTION April 18, 2017
COUNTY / MUNICIPALITY Fulton
PRECINCT SS25

TIME LAST VOTER VOTED _____

NUMBER OF REGISTERED VOTERS IN PRECINCT _____

DIRECT RECORD ELECTRONIC VOTING MACHINE RECAP

SECTION A: RECORD EACH UNIT

DRE UNIT NUMBER	Before Polls Open SEAL NUMBER	Before Polls Open COUNT NUMBER	After Polls Close SEAL NUMBER	After Polls Close COUNT NUMBER
113136	594161	0	1533872	104
123463	594110	0	1470276	101
110009	594746	0	1470277	64
143544	594763	0	1516529	[illegible]

SECTION B: TOTAL OF ALL VOTES CAST (ALL UNITS COMBINED) 486

SECTION C: NUMBERED LISTS and VOTER CERTIFICATES

ExpressPoll (See ExpressPoll Recap)		Supplemental		Total Voter's Certificates	
Democratic Primary		Democratic Primary		Democratic Primary	
Republican Primary		Republican Primary		Republican Primary	
General/Special		General/Special		General/Special	
Total (a)	477	**Total (b)**	0	**Total (c)**	477

SECTION D: TOTAL NUMBER OF PERSONS VOTING AS SHOWN BY:

1. Results Tapes (or Accumulator Tape Results) (Total from Section B above) = 486
2. "Voters Marked" (See ExpressPoll Recap) 477 + Supplemental List 0 = 477
3. Numbered Lists on ExpressPoll **(a)** 477 + Supplemental **(b)** 0 = 477
4. Voter's Certificates **(c)** = 477

NOTE: Numbers from D1, D2, D3, and D4 should match. If not, explain difference here:
1 Encoder approved by Kenesha 1 Absentee spoiled
1 vote cast by wrong voter and issued.

ram _____

We, the undersigned Managers, hereby certify that the above is a true and correct accounting on this the 18th day of April, 2014. **SIGNED IN TRIPLICATE**

Marilyn [illegible] — Manager
[illegible] — Assistant Manager
[illegible] — Assistant Manager

MARKS DECLARATION

Form RS-DRE-10

Exhibit 2.2
Fulton County Polling Place Recap Sheet Discrepancy
June 20, 2017 (Congressional District 6 Runoff)
Polling Place RW20

Note: The number of voters applying to vote at the polling place should reconcile to the number of ballots cast and number of votes reported with few, if any, reconciling items. The example recap sheet shows unreconciled differences. The number of voter certificates (voters voting) should be equal to the number of ballots cast.

Information on Recap Sheet:

Reported ballots cast per DRE results tape=347

Reported number of voter certificates (voters voting)= 362

Reported number of voters recorded in electronic pollbook=345

ELECTION: (Check One)
- ☐ General
- ☑ Primary
- ☐ Runoff (if applicable)
- ☐ Special
- ☐ Presidential Preference Primary

USE BALL POINT PEN
Bear Down – You Are Making Three Copies

WHITE sheet to Secretary of State
YELLOW sheet to Superintendent
PINK sheet to Clerk of Superior Court or Municipal Clerk

DATE OF ELECTION June 20, 2017
COUNTY /MUNICIPALITY Fulton
PRECINCT B1020

TIME LAST VOTER VOTED 7:33

NUMBER OF REGISTERED VOTERS IN PRECINCT 2057

DIRECT RECORD ELECTRONIC VOTING MACHINE RECAP

SECTION A: RECORD EACH UNIT

DRE UNIT NUMBER	Before Polls Open SEAL NUMBER	Before Polls Open COUNT NUMBER	After Polls Close SEAL NUMBER	After Polls Close COUNT NUMBER
109383	0663590	✓	1557723	45
112742	0663574	✓	1557722	70
122453	0663547	✓	1557726	19
122712	0663561	✓	1557725	52
125768	0663589	✓	1557724	85
145747	0663574	✓	1557727	6

SECTION B: TOTAL OF ALL VOTES CAST (ALL UNITS COMBINED) 347

SECTION C: NUMBERED LISTS and VOTER CERTIFICATES

ExpressPoll (See ExpressPoll Recap)	Supplemental	Total Voter's Certificates
Democratic Primary	Democratic Primary	Democratic Primary 362
Republican Primary	Republican Primary	Republican Primary
General/Special	General/Special	General/Special
Total (a) 345	Total (b) 0	Total (c) 362

SECTION D: TOTAL NUMBER OF PERSONS VOTING AS SHOWN BY:

1. Results Tapes (or Accumulator Tape Results) (Total from Section B above) = 347
2. "Voters Marked" (See ExpressPoll Recap) 345 + Supplemental List 0 = 345
3. Numbered Lists on ExpressPoll (a) _____ + Supplemental (b) _____ = _____
4. Voter's Certificates (c) = 362

NOTE: Numbers from D1, D2, D3, and D4 should match. If not, explain difference here: Machine went down several times Number were off.

We, the undersigned Managers, hereby certify that the above is a true and correct accounting on this the 20th day of June, 2017. SIGNED IN TRIPLICATE

Manager | Assistant Manager | Assistant Manager

MARKS DECLARATION
Form RS-DRE-10

Exhibit 2.3

Fulton County Polling Place Recap Sheet Discrepancy
April 18, 2017 (Congressional District 6 Special Election)
Polling Places SS02A/B, SS19A/B, SS20, SS26 (combined)

Note: The number of voters applying to vote at the polling place should reconcile to the number of ballots cast and number of votes reported with few, if any, reconciling items. The example recap sheet shows unreconciled differences. The number of ballots cast should not exceed the number of voters applying to vote.

Information on Recap Sheet:

Reported ballots cast per DRE results tape= 1,962

Reported number of voter certificates (voters voting)= not reported, unknown

Electronic Pollbook voter count (voters voting)= 1,790

ELECTION: (Check One)
- ☐ General
- ☐ Primary
- ☐ Runoff (if applicable)
- ☒ Special
- ☐ Presidential Preference Primary

1853

DATE OF ELECTION April 18, 2017
COUNTY / MUNICIPALITY Fulton
PRECINCT SS02A/B, SS19A/B, SS20 & SS24

USE BALL POINT PEN
Bear Down – You Are Making Three Copies

WHITE sheet to Secretary of State
YELLOW sheet to Superintendent
PINK sheet to Clerk of Superior Court or Municipal Clerk

TIME LAST VOTER VOTED 7:05

NUMBER OF REGISTERED VOTERS IN PRECINCT 1962

DIRECT RECORD ELECTRONIC VOTING MACHINE RECAP

SECTION A: RECORD EACH UNIT

DRE UNIT NUMBER	Before Polls Open SEAL NUMBER	Before Polls Open COUNT NUMBER	After Polls Close SEAL NUMBER	After Polls Close COUNT NUMBER
124235	0594784	0	1475496	16
125814	0594762	0	1475343	51
111569	0594788	0	1475497	98
125312	0594795	0	1475342	101
117219	0594785	0	1475495	112
102454	0594797	0	1475350	84
124548	0594776	0	1475349	73
141133	0594773	0	1475344	40
111128	0594781	0	1533856	22
125241	0594758	0	1475347	3
114412	0594789	0	1475346	24
116629	0594771	0	1475341	52
124634	0594796	0	1475567	40
117214	0594766	0	1475568	113
112310	0594767	0	1475570	160

SECTION B: TOTAL OF ALL VOTES CAST (ALL UNITS COMBINED) _____

SECTION C: NUMBERED LISTS and VOTER CERTIFICATES

ExpressPoll (See ExpressPoll Recap)	Supplemental	Total Voter's Certificates
Democratic Primary _____	Democratic Primary _____	Democratic Primary _____
Republican Primary _____	Republican Primary _____	Republican Primary _____
General/Special _____	General/Special _____	General/Special _____
Total (a) _____	**Total (b)** _____	**Total (c)** _____

SECTION D: TOTAL NUMBER OF PERSONS VOTING AS SHOWN BY:

1. Results Tapes (or Accumulator Tape Results) (Total from Section B above) = 1962
2. "Voters Marked" (See ExpressPoll Recap) 1790 + Supplemental List 1 = 1791
3. Numbered Lists on ExpressPoll **(a)** 1790 + Supplemental **(b)** 0 = _____
4. Voter's Certificates **(c)** = _____

NOTE: Numbers from D1, D2, D3, and D4 should match. If not, explain difference here: _____
Appears the express poll c.d. not sync.

We, the undersigned Managers, hereby certify that the above is a true and correct accounting on this the 18 day of Apr, 2017. **SIGNED IN TRIPLICATE**

Manager _____ Assistant Manager _____ Assistant Manager _____

MARKS DECLARATION

Form RS-DRE-10

ELECTION: (Check One)
- ☐ General
- ☐ Primary
- ☐ Runoff (if applicable)
- ☑ Special
- ☐ Presidential Preference Primary

2 of 3

DATE OF ELECTION April 18, 2017
COUNTY / MUNICIPALITY Fulton
PRECINCT SS02 A/B, SS19 A/B, SS20 & SS24

USE BALL POINT PEN
Bear Down – You Are Making Three Copies

WHITE sheet to Secretary of State
YELLOW sheet to Superintendent
PINK sheet to Clerk of Superior Court or Municipal Clerk

TIME LAST VOTER VOTED 7:05

NUMBER OF REGISTERED VOTERS IN PRECINCT _____

DIRECT RECORD ELECTRONIC VOTING MACHINE RECAP

SECTION A: RECORD EACH UNIT

DRE UNIT NUMBER	Before Polls Open SEAL NUMBER	Before Polls Open COUNT NUMBER	After Polls Close SEAL NUMBER	After Polls Close COUNT NUMBER
1[illegible]15	0594769	0	1475563	86
1[illegible]79	0594765	0	1475562	64
146141	0594793	0	1533852	105
116148	0594794	0	1475566	90
1[illegible]11	0594763	0	1475494	127
1[illegible]427	0594798	0	1434919	67
159198	0594787	0	1475564	33
111136	0594760	0	1475569	13
111544	0594768	0	1434911	1
1[illegible]504	0594772	0	1475565	14
114015	0594743	0	1475376	30
1442[illegible]7	0594745	0	1475561	96
128136	0594754	0	1475491	63
112101	0594744	0	1475378	84
145120	0594777	0	1475375	88

SECTION B: TOTAL OF ALL VOTES CAST (ALL UNITS COMBINED) _____

SECTION C: NUMBERED LISTS and VOTER CERTIFICATES

ExpressPoll (See ExpressPoll Recap)	Supplemental	Total Voter's Certificates
Democratic Primary _____	Democratic Primary _____	Democratic Primary _____
Republican Primary _____	Republican Primary _____	Republican Primary _____
General/Special _____	General/Special _____	General/Special _____
Total (a) _____	**Total (b)** _____	**Total (c)** _____

SECTION D: TOTAL NUMBER OF PERSONS VOTING AS SHOWN BY:

1. Results Tapes (or Accumulator Tape Results) (Total from Section B above) = 1962
2. "Voters Marked" (See ExpressPoll Recap) _____ + Supplemental List _____ = 1791
3. Numbered Lists on ExpressPoll **(a)** _____ + Supplemental **(b)** _____ = _____
4. Voter's Certificates **(c)** = _____

NOTE: Numbers from D1, D2, D3, and D4 should match. If not, explain difference here: _____

E.P. did not sync.

We, the undersigned Managers, hereby certify that the above is a true and correct accounting on this the 18 day of April, 2017. **SIGNED IN TRIPLICATE**

Manager _____ **Assistant Manager** _____ **Assistant Manager** _____

MARKS DECLARATION

Form RS-DRE-10

ELECTION: (Check One)
- ☐ General
- ☐ Primary
- ☐ Runoff (if applicable)
- ☑ Special
- ☐ Presidential Preference Primary

803

DATE OF ELECTION April 18, 2017
COUNTY / MUNICIPALITY Fulton
PRECINCT SS02 A/B, SS19 A/B, SS20 & SS24

USE BALL POINT PEN
Bear Down – You Are Making Three Copies

WHITE sheet to Secretary of State
YELLOW sheet to Superintendent
PINK sheet to Clerk of Superior Court or Municipal Clerk

TIME LAST VOTER VOTED 7:05

NUMBER OF REGISTERED VOTERS IN PRECINCT _____

DIRECT RECORD ELECTRONIC VOTING MACHINE RECAP

SECTION A: RECORD EACH UNIT

DRE UNIT NUMBER	Before Polls Open SEAL NUMBER	Before Polls Open COUNT NUMBER	After Polls Close SEAL NUMBER	After Polls Close COUNT NUMBER
144260	0594732	0	1475345	8
107666	0594748	0	1475348	2

SECTION B: TOTAL OF ALL VOTES CAST (ALL UNITS COMBINED) _____

SECTION C: NUMBERED LISTS and VOTER CERTIFICATES

ExpressPoll (See ExpressPoll Recap)	Supplemental	Total Voter's Certificates
Democratic Primary _____	Democratic Primary _____	Democratic Primary _____
Republican Primary _____	Republican Primary _____	Republican Primary _____
General/Special _____	General/Special _____	General/Special _____
Total (a) _____	**Total (b)** _____	**Total (c)** _____

SECTION D: TOTAL NUMBER OF PERSONS VOTING AS SHOWN BY:

1. Results Tapes (or Accumulator Tape Results) (Total from Section B above) = 1792
2. "Voters Marked" (See ExpressPoll Recap) 1790 + Supplemental List 1 = 1791
3. Numbered Lists on ExpressPoll **(a)** 1792 + Supplemental **(b)** _____ = _____
4. Voter's Certificates **(c)** = _____

NOTE: Numbers from D1, D2, D3, and D4 should match. If not, explain difference here: _____
Applus the EP. did not sync

We, the undersigned Managers, hereby certify that the above is a true and correct accounting on this the 18 day of April, 2017. **SIGNED IN TRIPLICATE**

Manager _____ Assistant Manager _____ Assistant Manager _____

MARKS DECLARATION

Form RS-DRE-10

Exhibit 2.4
Fulton County Polling Place Recap Sheet Discrepancy
December 5, 2017 (Atlanta Municipal Election Runoff)
Polling Place 07F 08L

Note: The number of voters applying to vote at the polling place should reconcile to the number of ballots cast and number of votes reported with few, if any, reconciling items. The example recap sheet shows unreconciled differences. The number of ballots cast should not exceed than the number of voters applying to vote.

Information on Recap Sheet:

Reported ballots cast per DRE results tape=486

Reported number of voter certificates (voters voting)= 477

Reported election day votes for CD6 per official results= 479 (computed)
(http://results.enr.clarityelections.com/GA/Fulton/67378/Web02/#/)

ELECTION: (Check One)
- ☑ General
- ☐ Primary
- ☑ Runoff (if applicable)
- ☑ Special
- ☐ Presidential Preference Primary

USE BALL POINT PEN
Bear Down – You Are Making Three Copies

WHITE sheet to Secretary of State
YELLOW sheet to Superintendent
PINK sheet to Clerk of Superior Court or Municipal Clerk

DATE OF ELECTION Dec. 5, 2017
COUNTY /MUNICIPALITY Fulton
PRECINCT 01F & 082

TIME LAST VOTER VOTED _____

NUMBER OF REGISTERED VOTERS IN PRECINCT _____

DIRECT RECORD ELECTRONIC VOTING MACHINE RECAP

SECTION A: RECORD EACH UNIT

DRE UNIT NUMBER	Before Polls Open SEAL NUMBER	Before Polls Open COUNT NUMBER	After Polls Close SEAL NUMBER	After Polls Close COUNT NUMBER
128968	0613368	0	1603475	338
112864	0613372		1594345	262
111085	0613346		1603474	249
116942	0613351		1603448	163
125762	0613358		1603471	149
115304	0613362		1594353	88
110009	0613374		1594344	44
143949	0613400		1594348	32
125613	0613394		1603472	18
126823	0613340		1594592	12
137606	0613385		1594349	9

SECTION B: TOTAL OF ALL VOTES CAST (ALL UNITS COMBINED) 1364

SECTION C: NUMBERED LISTS and VOTER CERTIFICATES

ExpressPoll (See ExpressPoll Recap)		Supplemental		Total Voter's Certificates	
Democratic Primary	/	Democratic Primary	/	Democratic Primary	/
Republican Primary	/	Republican Primary	/	Republican Primary	
General/Special	1161	General/Special		General/Special	1388
Total (a)	1161	Total (b)	0	Total (c)	1388

SECTION D: TOTAL NUMBER OF PERSONS VOTING AS SHOWN BY:

1. Results Tapes (or Accumulator Tape Results) (Total from Section B above) = 1364
2. "Voters Marked" (See ExpressPoll Recap) 1161 + Supplemental List 0 = 1161
3. Numbered Lists on ExpressPoll (a) 0 + Supplemental (b) 0 = 0
4. Voter's Certificates (c) = 1388

NOTE: Numbers from D1, D2, D3, and D4 should match. If not, explain difference here: Issues w/ express polls shutting down, losing sync connection, moving slow & freezing up.

We, the undersigned Managers, hereby certify that the above is a true and correct accounting on this the 5th day of December, 2017. **SIGNED IN TRIPLICATE**

Manager _____ Assistant Manager _____ Assistant Manager _____

MARKS DECLARATION
Form RS-DRE-10

EXHIBIT 3

A	B	C	D	E
County	Registered Voters	Ballots Cast	Voter Turnout	
Habersham North	7740	1747	22.57 %	
Habersham South	5113	969	18.95 %	
Demorest	4135	816	19.73 %	
Town of Mount Airy	650	135	20.77 %	
City of Baldwin	838	102	12.17 %	
Mud Creek	276	670	242.75 %	
Amys Creek	1355	309	22.80 %	
Total:	20107	4748	23.61 %	

	A	B	C	D
1	Precinct	Registered Voter	Ballots Cast	Voter Turnout
2	01A	2714	2221	81.83 %
3	01B	3337	2748	82.35 %
4	01C	1120	620	55.36 %
5	01D	430	307	71.40 %
6	01E	4652	3462	74.42 %
7	01F	981	482	49.13 %
8	01H	661	419	63.39 %
9	01J	2030	1265	62.32 %
10	01P	1000	615	61.50 %
11	01R	1107	581	52.48 %
12	01S	1391	848	60.96 %
13	01T	1196	785	65.64 %
14	02A	3211	2450	76.30 %
15	02B	2895	1294	44.70 %
16	02C	1725	1295	75.07 %
17	02D	3582	2591	72.33 %
18	02E	1733	1466	84.59 %
19	02F1	2589	2080	80.34 %
20	02F2	669	491	73.39 %
21	02G	2959	2375	80.26 %
22	02J	1934	2219	114.74 %
23	02K	1246	1027	82.42 %
24	02L1	4934	3790	76.81 %
25	02L2	971	746	76.83 %
26	02S	620	447	72.10 %
27	02W	422	301	71.33 %
28	03A	1673	803	48.00 %
29	03B	494	208	42.11 %
30	03C	1294	780	60.28 %
31	03D	837	416	49.70 %

EXHIBIT 4

Paste

A1 | U.S. Representative, District 6

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1																	
2			TOM PRICE (I)							RODNEY STOOKSBURY							
3	Precinct	Registered V	Election Day	Absentee by	Advance in P	Advance in P	Advance in P	Provisional	Total Votes	Election Day	Absentee by	Advance in P	Advance in P	Advance in P	Provisional	Total Votes	Total
4	02J	1934	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1
5	AP01A	1739	243	52	592	3	25	1	916	112	30	273	2	13	2	432	1348
6	AP01B	685	79	16	152	1	5	0	253	62	5	132	1	11	1	212	465
7	AP01C	1952	269	67	671	6	43	0	1056	120	28	314	8	37	0	507	1563
8	AP01D	713	86	21	146	6	27	0	286	69	15	143	3	13	0	243	529
9	AP02B	352	24	55	62	3	5	0	149	11	32	27	2	7	0	79	228
10	AP03	619	69	1	38	2	8	0	118	136	3	87	14	38	1	279	397
11	AP04A	1472	238	63	80	3	493	1	878	74	15	47	3	197	1	337	1215
12	AP04B	364	54	12	13	0	127	0	206	19	4	17	1	62	0	103	309
13	AP05	3956	750	132	1288	7	32	2	2211	238	56	640	3	5	4	946	3157

MARKS DECLARATION

DECLARATION OF LAURIE ADERHOLT MITCHELL

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

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRIAN P. KEMP, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

DECLARATION OF LAURIE ADERHOLT MITCHELL

LAURIE ADERHOLT MITCHELL hereby declares as follows:

1. I am have been a Georgia voter since 2015 and am currently registered to vote at 408 E. Wesley Road NE, Atlanta, GA 30305. I have been continuously registered to vote at this address since June 20, 2015.
2. I have not made changes to my voter registration while living at this address.
3. I reside with my husband Mark Mitchell, who is also registered to vote at the above address, and has been continuously registered at this address since February 10, 2014.

4. On or about July 18, 2018, I was surprised to receive a new voter registration card in the mail. A copy is attached (Exhibit A).
5. I noticed that my polling place had changed from my traditional polling place of Cathederal of St. Philip at 2744 Peachtree Road to Sutton Middle School at 2875 Northside Drive.
6. My husband stated to me that he received no such notice.
7. I read reports on social media of various voting problems during the July 24, 2018 runoff with voters' registration records showing discrepancies in pollbooks when they attempted to vote.
8. Based on the concerning reports, I reviewed my registration card again and on July 19, 2018 went to My Voter Page on the Secretary of State's website at (https://www.mvp.sos.ga.gov/MVP/mvp.do) to verify that the card I received in the mail matched the online information. (Exhibit B) All information matched.
9. However, I noticed that not only had the precinct voting location changed but my precinct assignment had changed to 08H from 07F.
10. On July 19, 2018, both my husband and I checked his voter registration on My Voter Page and found that his registration had

remained at Precinct 07F with the same polling location at St. Philip's Cathedral. (Exhibit C)

11. I reviewed both my husband's and my registration information on My Voter Page and noted that I am assigned to City Council District 8, while he is assigned to City Council District 7, although the City Council District maps appear to show that we live in District 7.
12. I plan to vote in the November 2018 election and am concerned that I may be given an inaccurate ballot, or that my name may not be found in the pollbook, or that I will be otherwise disenfranchised.
13. After reading of reports of widespread errors in the pollbooks, I am also concerned about the impact of such discrepancies on the election as a whole, and the impact of widespread errors on voter confidence and voter turnout.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, July 30, 2018.

Laurie Aderholt Mitchell

EXHIBIT A

ATTENTION: This is your NEW Voter Registration Precinct Card. It replaces any other Voter Card you currently have in your possession. Keep for your records.
(Cut or fold on the dotted line for wallet card)

If you change your address within the county, complete this form and mail to the return address on the front of this card.

Note: Change of address must be submitted at least 30 days preceeding any election.

If you move to another county or if there is a change in your legal name, you must complete a new voter registration application in order to remain qualified to vote.

This card may not be used as evidence to prove United States Citizenship or as identification to vote. (ref.1996 United States Public Law 104-99)

Fold Here

YOUR NEW **RESIDENCE** ADDRESS **WITHIN** COUNTY (Please Print)

Number Street Apartment

City Zip Code

Mailing Address (If different)

City Zip Code

Daytime Telephone Date

VOTER'S SIGNATURE

From the Secretary of State website, www.sos.ga.gov, a registered voter with a valid Georgia driver's license or identification card issued by the GA Department of Driver Services may change his or her name or address using Online Voter Registration. You may also access Online Voter Registration by downloading the GA Votes app.

Visit our website @ www.mvp.sos.ga.gov/MVP, download the GA Votes app or contact your local registrar's office.

For Android

For Apple

VOTER REGISTRATION OFFICE
130 PEACHTREE STREET 2186
SW
ATLANTA GA 30303 - 3460
PHONE: 404-612-7020

FIRST CLASS MAIL
U.S. POSTAGE PAID
Atlanta, GA
PERMIT No: **2604**

RETURN SERVICE REQUESTED

REG. DATE 06/20/2015
ISSUE DATE 06/25/2018
REG. No. 02559347

FULTON COUNTY PRECINCT CARD
SIGN CARD AND KEEP FOR YOUR RECORDS

PRECINCT NAME: 08H
POLLING PLACE: SUTTON MIDDLE SCHOOL
2875 NORTHSIDE DRIVE NW , ATLANTA GA 30305 - 0000

CITY PRECINCT NAME: 08H
POLLING PLACE: SUTTON MIDDLE SCHOOL
2875 NORTHSIDE DRIVE NW , ATLANTA GA 30305 - 0000

VOTING DISTRICTS:

005	039	054	ATLA	3	08	4
CONG	SENATE	HOUSE	JUD	COMM	CITYL	MUNIB

LAURIE ADERHOLT MITCHELL
408 E WESLEY RD NE
ATLANTA GA 30305 - 3826

EXHIBIT B

MVP

MY VOTER PAGE
GEORGIA SECRETARY OF STATE BRIAN P. KEMP

Corporations | Elections | News Room | Professional Licensing Boards | Securities | Charities

My Voter Page

Voter Information

LAURIE ADERHOLT MITCHELL
408 WESLEY RD NW
ATLANTA, GA, 30305
Race: White not of Hispanic Origin
Gender: Female Status: Active
Registration Date: 06/20/2015

Change Voter Information

Click Here for Sample Ballots

Polling Place for State, County, and Municipal Elections

Precinct 08H
SUTTON MIDDLE SCHOOL
2875 NORTHSIDE DRIVE NW
ATLANTA, GA, 30305 - 0000
Election Day polling place hours are 7:00 am - 7:00 pm.

Directions to Polling Place

Click Here for Early Voting Locations and Times
Click Here for Municipal Polling Place

NOTE: Non-specific rural addresses may not be available.

Absentee Ballot Request Information

If you prefer to vote off-site, mail or fax your absentee ballot application to your county registrar.

Click Here for an Absentee Ballot Application

Click here for Absentee Ballot status

Your Elected Officials

Candidates Elected:	Officials Elected Statewide
District Maps:	Congressional District Maps
U.S. Congress:	District 005
Georgia Senate:	District 039
Georgia House:	District 054

Click Here for Qualified Candidates

Check your Provisional Ballot Status

Please Note: Polling places are subject to change. Always check your designated polling place location via this website prior to going to vote.

Newly Registered Voters: Please review your registration date which is located under your name and address above. You must be registered on or before the established deadlines to vote in upcoming elections. Please view the current election calendar to confirm the first election in which you will be eligible to vote.

Print / Email Precinct Card | Back

Georgia Voter ID
Learn more about Georgia Voter Identification Requirements

Stop Voter Fraud
Do Your Part to Help Ensure Secure and Fair Georgia Elections

Elections Division
Georgia Secretary of State's Elections Division

Elections Advisory Council
Share Your Ideas to Help Strengthen Georgia Elections

Georgia VoteSafe
Learn more about the Georgia VoteSafe Program

EXHIBIT C

MVP

MY VOTER PAGE
GEORGIA SECRETARY OF STATE BRIAN P. KEMP

Corporations | Elections | News Room | Professional Licensing Boards | Securities | Charities

My Voter Page

Voter Information

MARK ALEXANDER MITCHELL
408 E WESLEY RD NE
ATLANTA, GA, 30305
Race: White not of Hispanic Origin
Gender: Male Status: Active
Registration Date: 02/10/2014

Change Voter Information

Click Here for Sample Ballots

Polling Place for State, County, and Municipal Elections

Precinct 07F
CATHEDRAL OF SAINT PHILIP
2744 PEACHTREE RD NW
ATLANTA, GA, 30305 - 2937
Election Day polling place hours are 7:00 am - 7:00 pm.

Directions to Polling Place

Click Here for Early Voting Locations and Times
Click Here for Municipal Polling Place

NOTE: Non-specific rural addresses may not be available.

Absentee Ballot Request Information

If you prefer to vote off-site, mail or fax your absentee ballot application to your county registrar.

Click Here for an Absentee Ballot Application

Click here for Absentee Ballot status

Your Elected Officials

Candidates Elected:	Officials Elected Statewide
District Maps:	Congressional District Maps
U.S. Congress:	District 005
Georgia Senate:	District 039
Georgia House:	District 054

Click Here for Qualified Candidates

Check your Provisional Ballot Status

Georgia Voter ID
Learn more about Georgia Voter Identification Requirements

Stop Voter Fraud
Do Your Part to Help Ensure Secure and Fair Georgia Elections

Elections Division
Georgia Secretary of State's Elections Division

Elections Advisory Council
Share Your Ideas to Help Strengthen Georgia Elections

Georgia VoteSafe
Learn more about the Georgia VoteSafe Program

Please Note: Polling places are subject to change. Always check your designated polling place location via this website prior to going to vote.

Newly Registered Voters: Please review your registration date which is located under your name and address above. You must be registered on or before the established deadlines to vote in upcoming elections. Please view the current election calendar to confirm the first election in which you will be eligible to vote.

Print / Email Precinct Card | Back

DECLARATION OF REBECCA WILSON

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRIAN P. KEMP, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

DECLARATION OF REBECCA WILSON

REBECCA WILSON ("Declarant"), hereby declares as follows:

1. I serve as the Republican/Unaffiliated Chief Election Judge at Precinct 17–01, in Prince George's County, Maryland.

2. In Maryland, a bipartisan pair of "Chief Election Judges" supervises and manages the polling place on Election Day. I believe Georgia refers to these poll workers as "Supervisors."

3. I have been serving there since 2004. Until 2016, Maryland used Diebold's AccuVote Touchscreen Direct Recording Electronic (AV-TS DRE) voting machines, the same voting equipment that I understand Georgia uses. I supervised precinct pollworkers for the conduct of 11 elections in Precinct 17-01 using that equipment.

4. In 2016 Maryland switched to voter-marked paper ballots scanned by optical ballot scanners in the precinct. I have supervised 3 elections using paper ballots scanned by the new equipment.

5. The experience in my precinct is that the optical ballot-scanning system is far easier and faster to set up, manage, and close down after the polls are closed than the previous DRE equipment was. All of our election judges working in the polling place expressed to me that they believe paper ballots and optical scanning equipment are a more efficient approach to the conduct of the election.

SETTING UP THE POLLING PLACE

6. Since the switch to paper ballots in 2016, it is far easier for the poll workers under my supervision to set up the equipment on Election Day morning and to open the polls on time.

7. Under Maryland's procedures, setting up the DREs required numerous security, technical testing and preparation steps to be performed for each DRE. Our polling place had at least 11 and as many as 17 DREs deployed there, depending on anticipated turnout. Setting up each unit required 43 steps, as detailed in Chapter 10 of our former election judges manual (Exhibit A) for a total of 473 to 731 steps.

8. I have reviewed the Georgia pollworkers manual at https://georgiapollworkers.sos.ga.gov/Shared%20Documents/Georgia%20Poll%20Worker%20Training%20Manual.pdf and have concluded that the DRE set up and closing procedures are similar to the procedures used in my polling location until 2016.

9. Setting up the ballot-scanning equipment requires 32 steps to be performed for each of the 2 ballot scanners in our current configuration for paper ballots and optical scans, for a total of 64 steps. Setting up the accessible ballot-marking device (BMD) requires 18 steps for the one BMD in our precinct. (See Exhibit B, Chapters 11 & 12 of our current election judges manual.)

CLOSING DOWN THE EQUIPMENT

10. After switching to paper ballots in 2016, it was far easier for the pollworkers under my supervision to close down the equipment on Election Night and to obtain election results quickly.

11. Closing down the DREs required 40 steps to be performed for each DRE, for a total of 440 to 680 steps. Workers were required to print multiple copies of results tapes of each of the 11-17 DRE machines and then go through the cumbersome and time consuming process of shutting down, securing, and aggregating the results from each machine. These steps are detailed in Chapter 11 of our former election judge's manual. (See Exhibit C.)

12. Closing down the ballot-scanning equipment requires 29 steps to be performed for each of the two ballot scanners in our precinct, for a total of 58 steps. Closing the accessible ballot-marking device requires 9 steps for the one BMD in our precinct. These steps are detailed in Chapters 12 and 17 of our current election judge's manual. (See Exhibit D.)

ELECTION JUDGE TRAINING

13. Prince George's County requires four hours of training for each election judge before each election. This has been our long-standing training time requirement.

14. I have attended each of the four hour training sessions for the past 16 years.

15. The bulk of the training has not changed with the introduction of the new ballot-scanning system. Most of the training time is dedicated to polling place laws, rules, and procedures and to operation of the electronic pollbooks, which are not affected by the voting equipment used.

16. The training time that used to be dedicated to practice setting up, using, and closing down the DREs is now devoted instead to training election judges in paper ballot management and on instructing voters how to hand-mark their paper ballots, use the ballot-marking devices, and insert their ballots into the scanners. There were few questions and judges appeared to be quite comfortable with the change to paper ballots at the training session I attended.

17. Chief judges are also instructed in how to set up, manage, and close down the ballot scanners and the ballot-marking devices. I found these procedures to be relatively simple compared to the same procedures on DREs. My experience in the polling place on Election Day was consistent with the training that a paper ballot election is fairly simple to conduct.

SECURITY

18. In my role in supervising the polling place, I found it far easier to monitor the physical security of the ballot scanning system than the DRE system.

19. During the years we used DREs I knew that when I printed the "zero report" before voting opened that it was intended to indicate that the machine contained no votes, but provide no actual assurance. I was aware that bad actors could program the machines to print zeroes regardless of whether votes may have been pre-loaded into the machines.

20. In contrast, when we set up the ballot-scanning machine on Election Day morning, we can see with our own eyes that the ballot bin is empty and contains no voted ballots. The zero report printed from the DREs does not provide the same level of certainty.

21. With the DREs, each voter was left unattended at a voting machine for the amount of time it took them to cast their ballot, which could be up to 20 or 30 minutes depending upon the length of the ballot. If a voter had wanted to access the compartment of the machine where the memory card is stored, or cast multiple ballots with forged voter access cards, or manipulate the machine in other ways, the privacy screen on the machine would have generally prevented poll workers from seeing them do so.

22. By contrast, paper ballots and the ballot scanner are securely controlled, preventing anyone from accessing voted ballots or voting multiple ballots. Voters never have unattended access to the voted ballots or unvoted paper ballot stock or the ballot scanning

machine. An election judge is stationed at the ballot scanner all day and supervises each voter's brief interaction with the machine.

23. To receive a blank paper ballot, a voter must present to the election judge their Voter Authority Card (VAC), the check-in slip printed by the e-pollbook when the voter checked in. A blank paper ballot may not be issued without a valid VAC.

24. By contrast, the memory card compartment of the AV-TS DRE is locked with a commonly available key that is the same key used by every Diebold DRE, as well as by many other devices such as hotel minibars. This information has been widely published for many years.

25. Despite the enormous time and attention devoted to monitoring the physical security of the DREs, I believe that this is mostly "security theater." These precautions could not prevent or detect the most dangerous type of threat to the security of the machines: the threat of insider tampering with the software on which the machines operate. I feel confident that paper ballot security provides for verifiable and auditable results.

REDUCED VOTER CONFUSION AND INCONVENIENCE

26. Voters have expressed to me that they were very happy with the new paper balloting equipment. Voting went smoothly and quickly in my precinct and we experienced no wait times longer than 10 minutes at check-in during peak voting hours. Based on my experience, I would foresee no likelihood of confusion on the part of voters if they were required to switch from DRE to paper ballot voting.

27. In previous elections with our DREs we had documented wait times as long as 105 minutes in our polling place. (See Exhibit E.)

28. DRE machines occasionally freeze operations, have calibration problems, battery life issues, and experience other functional issues expected when running 15 year old computers.

Further Declarant sayeth not.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, August 1, 2018.

EXHIBIT A

Setting Up the Voting Units

Note: Touchscreen voting units can be placed on a table instead of on the unit's legs. A metal bracket is used to secure the touchscreen at a 90-degree angle. Voters can use the touchscreen voting unit to vote while sitting (wheelchair or folding chair). If the touchscreen voting unit is set up on the unit's legs instead of a table, the 90-degree touchscreen will still be accessible to most voters in a seated position.
To set a voting unit up on its legs:

1. With two people, place the voting unit upside down or on its side on the floor or table.

2. Locate the black securing latch connected to a flat metal support bar on the top leg assembly.

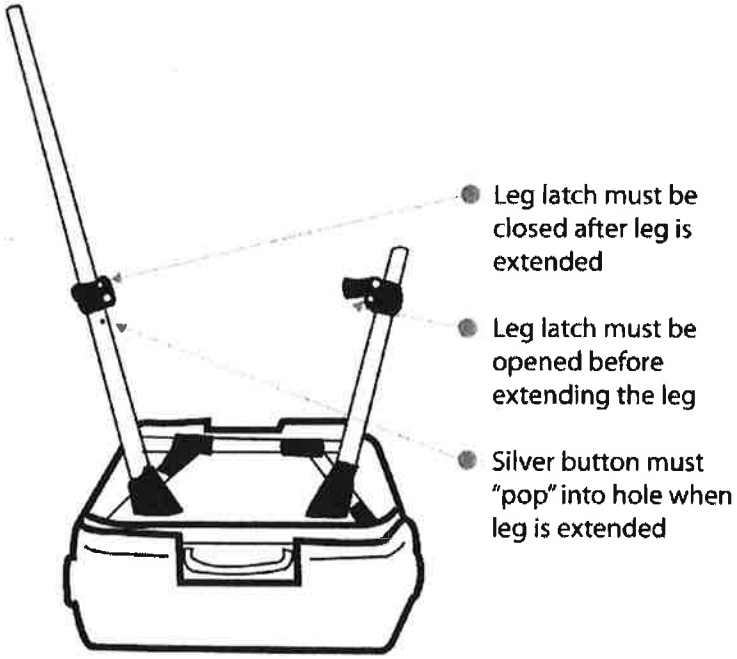
3. Release this latch.

4. Unfold the top leg until fully extended, and re-secure the black latch.

5. Release the smaller black securing latches on the end of each leg.

6. Extend each leg by pulling the lower leg assembly out until it locks and the silver button appears in the leg slot. If the silver button does not lock into the slot, you may need to twist the leg slightly to align the silver button with the slot. Do not over-twist the leg.

7. Lock the black securing latches.



8. Repeat steps 2-7 for the other legs.

9. With two people, lift the voting unit and stand it on all four legs.

10. When the voting unit is placed on the floor, gently pull the 4 legs outward for the widest stance and greatest stability.

11. Verify that each black securing latch is in the closed position.

    Note: Power cords are locked inside the metal blue box on top of the voting units.

12. Locate and insert the power cord into the left side of the voting unit and connect voting units according to the site survey. Follow the diagram below to daisy-chain the voting units.

Audio Ballot Equipment (VIBS - Visually Impaired Ballot Station)

Note: All voting units can be set up as VIBS (Visually Impaired Ballot Station) units with a keypad and headphones for voters who wish to use the audio ballot.

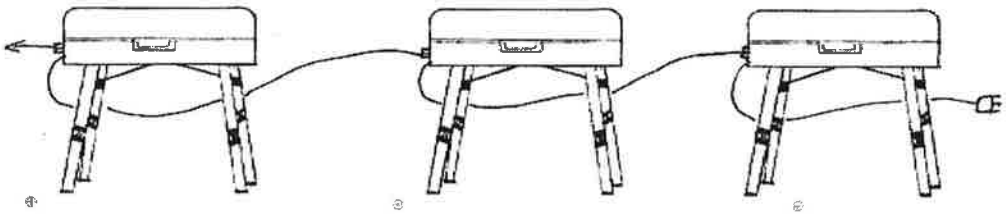
Note: The audio ballot equipment may have already been installed prior to delivery of the voting units. If not, follow the steps below.

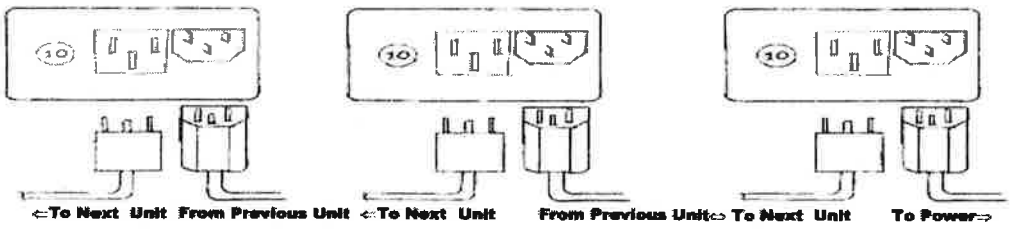
The keypad, headphones, and bracket are located in the supply bag (purple bag with red tag). The accessible voting unit is labeled with an orange tag.

1. Insert the keypad into the "Keypad" port on the right side of the voting unit. If already attached, check that it is tightly connected.

2. Insert the headphones into the "Audio" port on the right side of the voting unit. If already attached, check that it is tightly connected.

3. Secure the right side privacy screen.





⚠ **DON'T** daisy-chain more than 10 voting units together.

13. Plug the last power cord into the power strip, and plug the power strip into the wall. Turn power strip on.

Opening the Voting Units

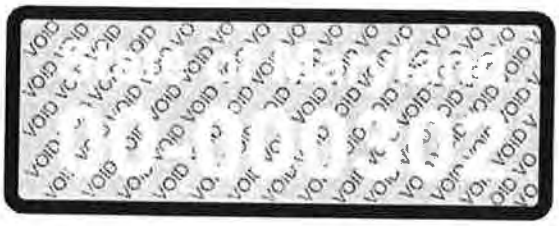
1. Verify that the number on the seal matches the number recorded on the *Voting System Integrity Report*. If the number does not match, call the local board of elections **immediately**.

2. Break the seal and place the broken seal into the Chief Judges' Case.

3. Locate the two latches by the black handle. Pull down the center of each latch and lift up the lid to the voting unit case.

4. Verify that the tamper tape covering the side compartment door is intact. If the word "Void" is visible (see image below) or there is no tape, call the local board of elections **immediately**.

Sample of intact tamper tape



Sample of voided tamper tape

5. Verify that the tamper tape number matches the number recorded on Page 1 of the *Voting System Integrity Report*. **Two election judges** must initial Page 1 of the *Voting System Integrity Report* to show that the number on **each** tamper tape was verified. **If the tamper tape number doesn't match, call the local board of elections immediately.**

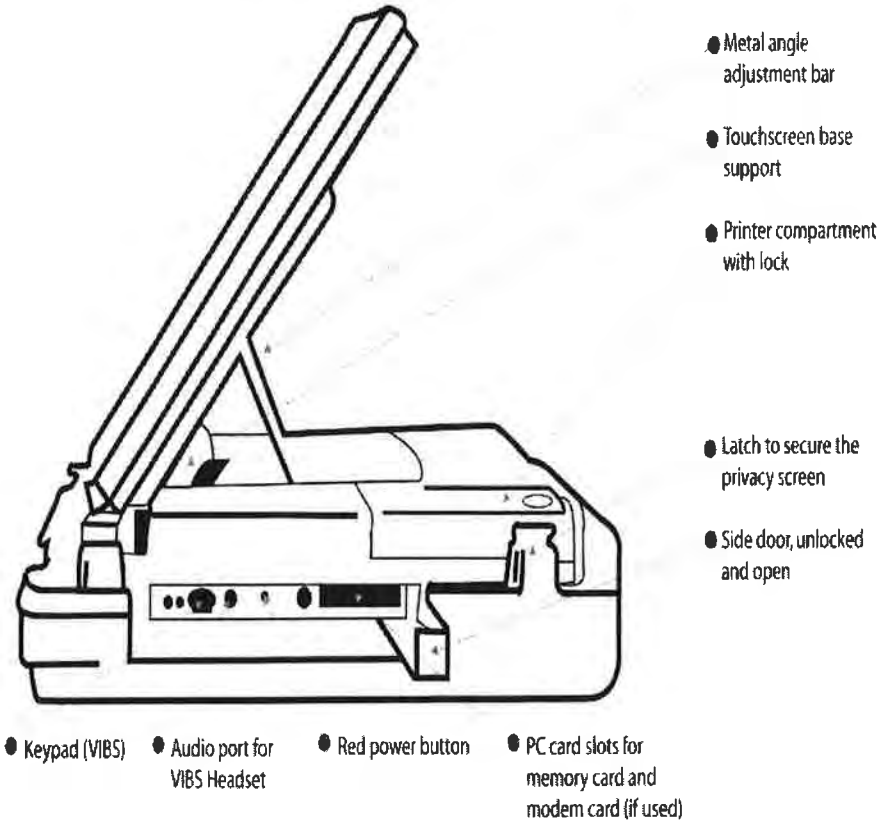
6. Push the internal power cord on the back left side of the voting unit to ensure that it is connected securely.

7. Extend both privacy screens (side panels) from the lid.

8. Snap the left privacy screen to the voting unit. Leave the right privacy screen unsnapped until you have printed the Zero Report.

9. Press the black button at the top of the touchscreen. Raise the touchscreen until you feel resistance from the touchscreen base support.

Note: Don't over-rotate the touchscreen unless you are setting up the accessible voting unit. If you over-rotate the touchscreen, the touchscreen base support will pop out of its slot. To get the touchscreen base support into its slot, press on it with a firm inward motion while lowering the touchscreen.



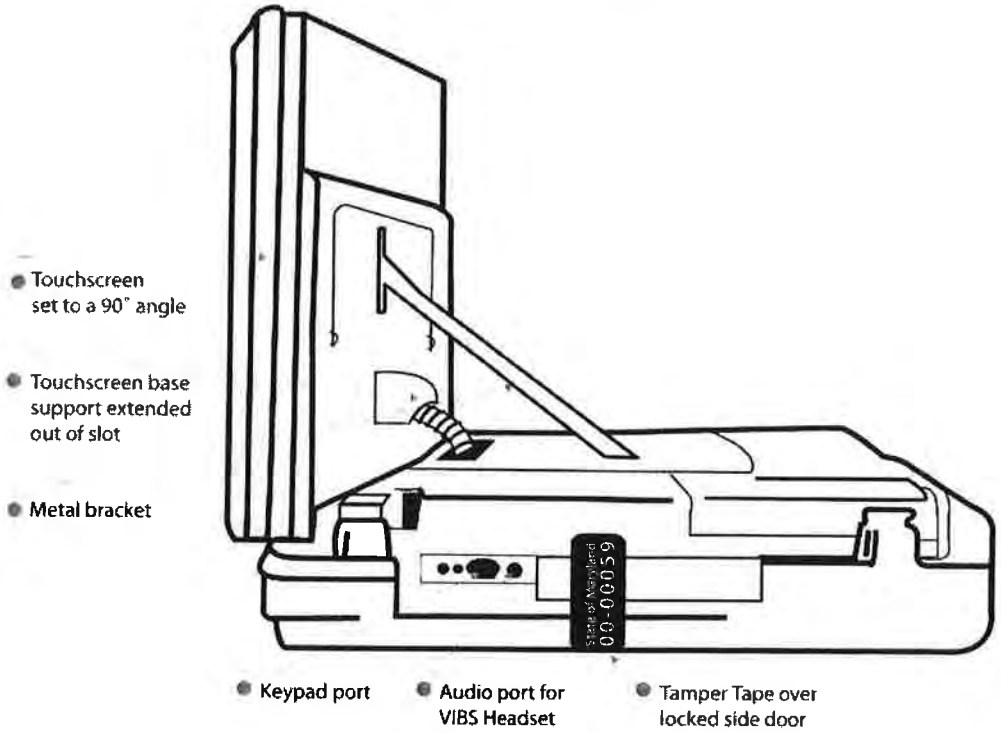
10. Lower the metal angle-adjustment bar under the touchscreen.

    A. To set the touchscreen at an angle for a voter who will stand while voting, allow the touchscreen to rest on the bar at an appropriate angle.

    B. To set the touchscreen at a 90-degree angle (for voters who will sit while voting):

    - Over-rotate the touchscreen so that the touchscreen base support pops out of its slot.
    - Insert the end of the metal bracket with the rectangular hole into the slot on the back of the touchscreen.
    - Insert the other end of the metal bracket into the slot on the base of the voting unit.
    - Verify that the touchscreen is stable in its 90-degree position.

Note: Be aware of glare on the touchscreens. If there is too much glare, adjust the touchscreen angle and/or, if practical, turn off overhead lights.



11. Remove the tamper tape from the side compartment and place the used tamper tape on the back of Page 1 of the *Voting System Integrity Report*.

12. Using the key, unlock the side compartment located on the right side of the unit and the printer compartment located on the top of the unit. The key is located in the Chief Judge's Case.

13. Make sure that the gray bar on the printer is lowered.

14. Press the red power button in the side compartment.

15. Once the unit starts up (about 45 seconds), the 1st Zero Report will automatically print.

16. Lock the side compartment door.

17. Verify that the following information appears correctly on the touchscreen:

    A. At the top center of the screen, verify the **current election**, **Election Day date, the county** and the **precinct number**.

B. Verify that the power bar at the bottom right of the screen is green and says "Charging." If the power bar is not green and "Charging," refer to **Chapter 12: Problems and Solutions**.

C. Verify that the **"Ballots"** number at the bottom of the screen is **zero**. Record that number on Page 1 of the *Voting System Integrity Report*.

D. Verify that the **"Tot"** number at the bottom of the screen **matches** the number on Page 1 of the *Voting System Integrity Report*.

Note: If any of the information in items A - D is incorrect, lower the screen and do not use the voting unit. Call the local board of elections **immediately**.

18. When the first Zero Report has been printed, verify that:

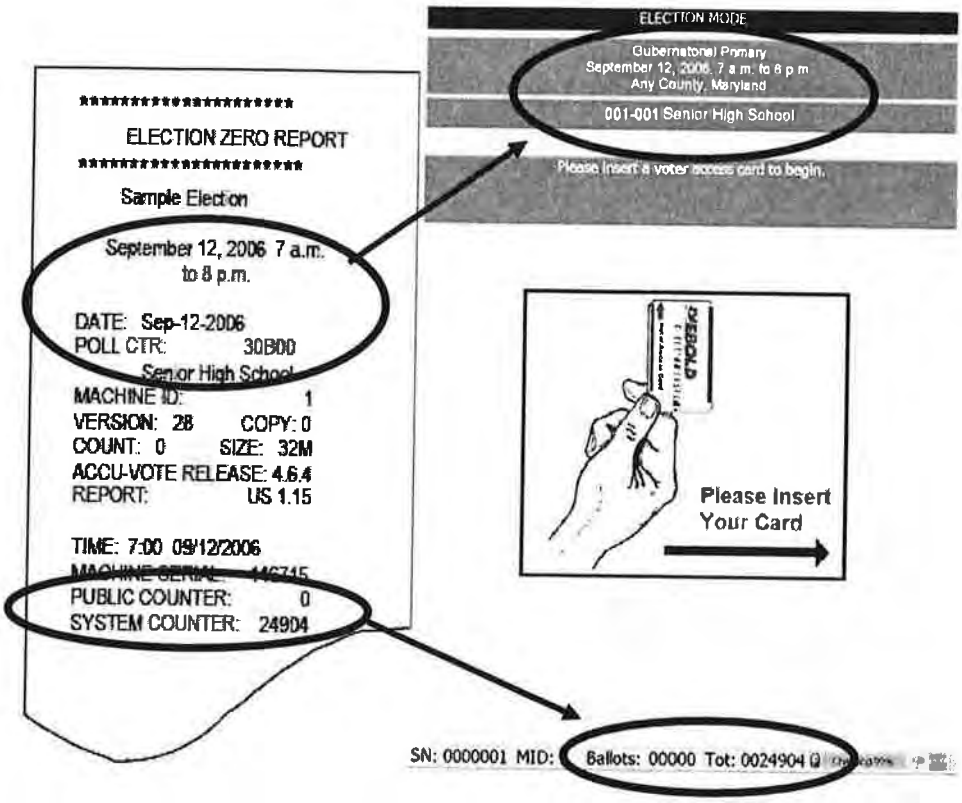
A. The date and precinct information on the report is correct;

B. The "Public Counter" on the report is zero and matches the "Ballots" number at the bottom of the screen;

C. The "System Counter" matches the "Tot" at the bottom of the screen; and

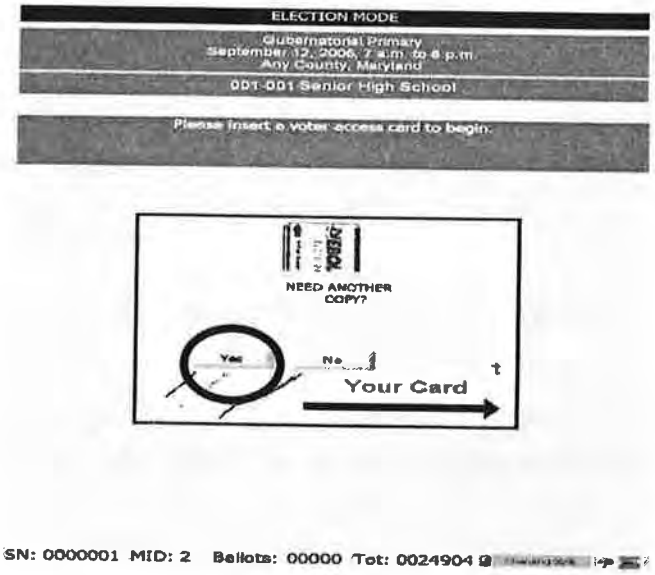
D. **All** contests on the report are zero.

Note: Notify the local board of elections **immediately** if there are errors on the Zero Report.



19. Tear off the 1st Zero Report. **Two election judges** must sign the Zero Report before posting it near the entrance to the polling place where the voters can see the report.

20. The "Need Another Copy?" message will automatically appear. Press "Yes."



21. A second Zero Report will print. **DON'T tear off the second Zero Report.** (The Totals Report printed at the end of election day **must** be attached to this Zero Report.) **Two election judges** must sign the second Zero Report.

⚠ Do **NOT** tear off the 2nd Zero Report!

22. The "Need Another Copy?" message will automatically appear again. If the second Zero Report printed correctly, press "No." If the second Zero Report did not print correctly (i.e. the paper jammed), reset the paper, and return to step 20.

23. The "Please Insert Your Card" screen will automatically appear.

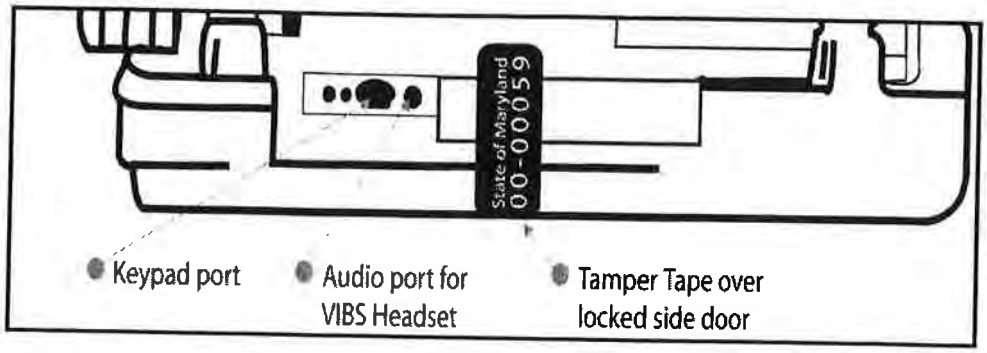
24. Roll up the second Zero Report and place it in front of the paper roll.

25. Lock the top printer compartment and verify that the side compartment is locked.

26. Locate the new tamper tape in the Chief Judges' Case.

27. Record the new tamper tape number on Page 1 of the *Voting System Integrity Report*.

28. Place the new tamper tape over the keyhole of the side compartment. The tamper tape must extend above and below the side compartment door. See the illustration below for the proper positioning of the tamper tape.



29. Secure the right side privacy screen.

⚠ Attach the container used to collect voter authority cards to the voting unit.

30. Locate the brown envelopes marked "Voter Authority Cards" in the sign bag (blue tote bag with blue tag). Write the precinct, ward, and voting unit number on the front of the envelope before attaching it securely to the back of the black top of the voting unit with duct tape.

Note: The next illustration shows how the voting system should look once set up and ready for voting.

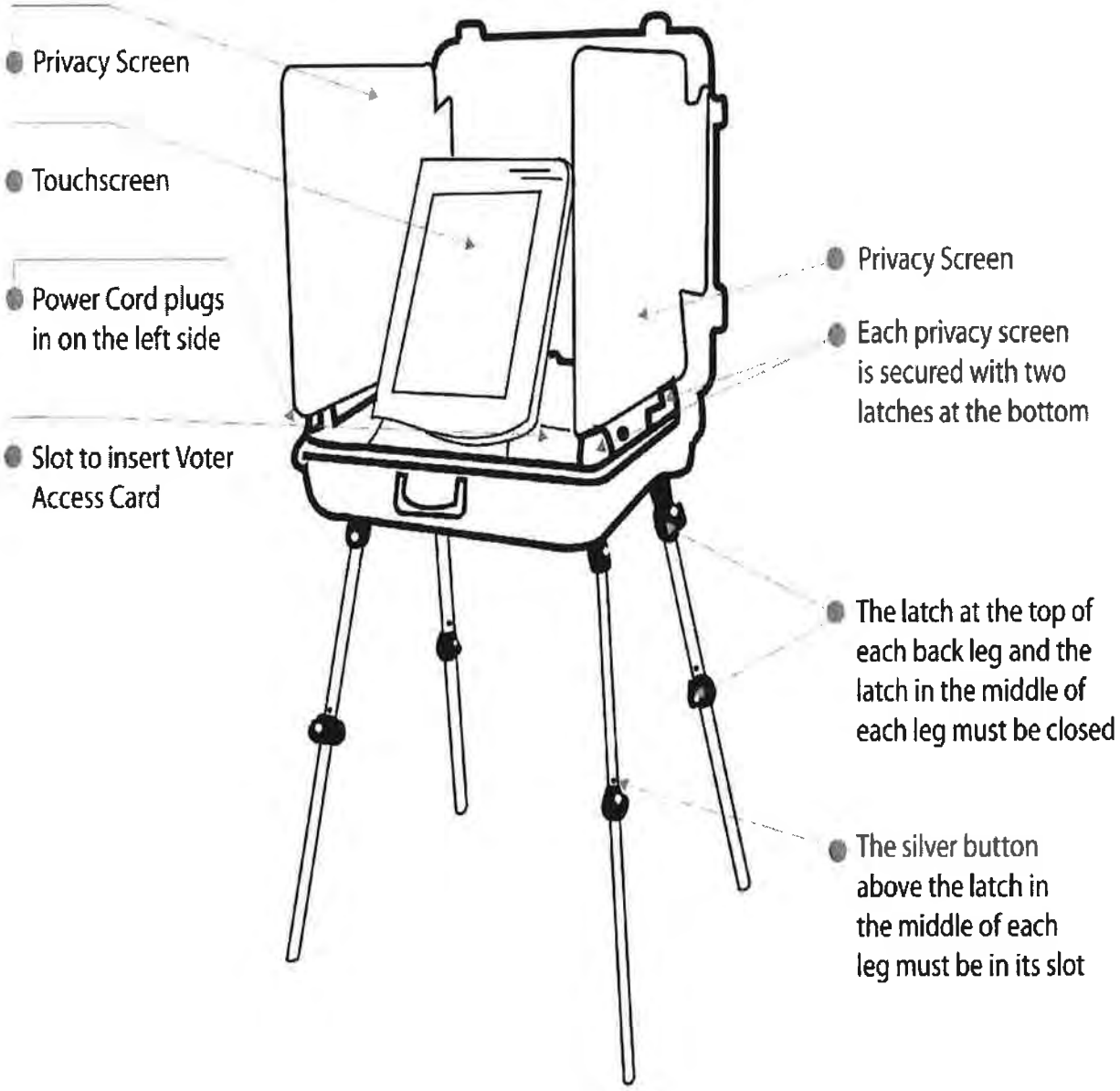

Privacy Screen
Touchscreen
Power Cord plugs in on the left side
Slot to insert Voter Access Card
Privacy Screen
Each privacy screen is secured with two latches at the bottom
The latch at the top of each back leg and the latch in the middle of each leg must be closed
The silver button above the latch in the middle of each leg must be in its slot

EXHIBIT B

Overview

Each precinct will receive at least one Scanning Unit. Large precincts may receive more than one Scanning Unit.

Poll Watchers may observe opening procedures.

⚠ **At least one voting judge must be stationed at the Scanning Unit at all times. Voting Judges may be rotated in and out of this position by Chief Judges during the day.**

Required Supplies

You will need the following supplies to open the Scanning Units:

Large Manila Envelope for collecting VACs

Scanning Unit key

Scanning Unit Integrity Report – Opening

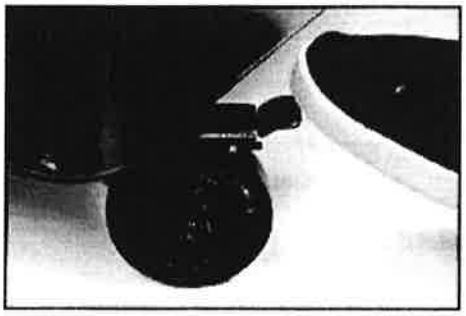
New tamper tape and green seals

Wire Cutters to break security seals on the outside of the Scanning Unit

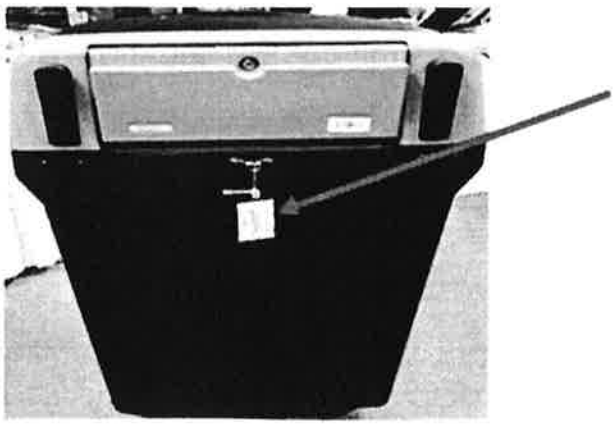
Scanning Unit Setup

1. Remove the Scanning Unit from the Transfer Cart (to prevent injury and damage, this should be done by at least two election judges). Roll the Scanning Unit to the location designated by precinct site survey.

2. Engage both parking brakes on the Scanning Unit by gently stepping on the metal tabs. They will snap into place. **Caution: The metal tabs are sharp.**



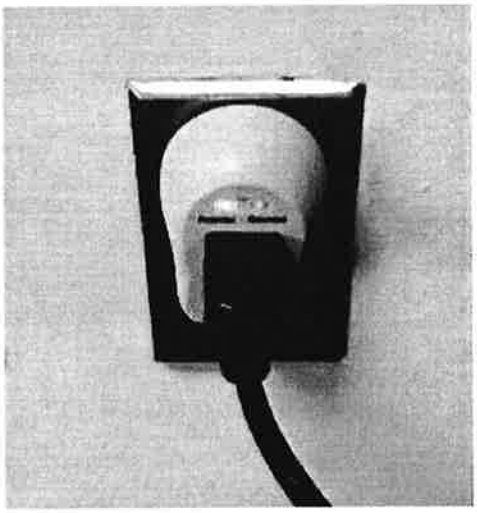
3. Confirm that the shipping label on the back of the Scanning Unit shows the correct polling place. If it does not, immediately notify the local board of elections.



4. Use the flat key to unlock the back door of the Scanning Unit, unwrap the power cord (with the grey surge protector attached) and plug the cord into an electrical outlet. **Leave the power cord compartment door open.**

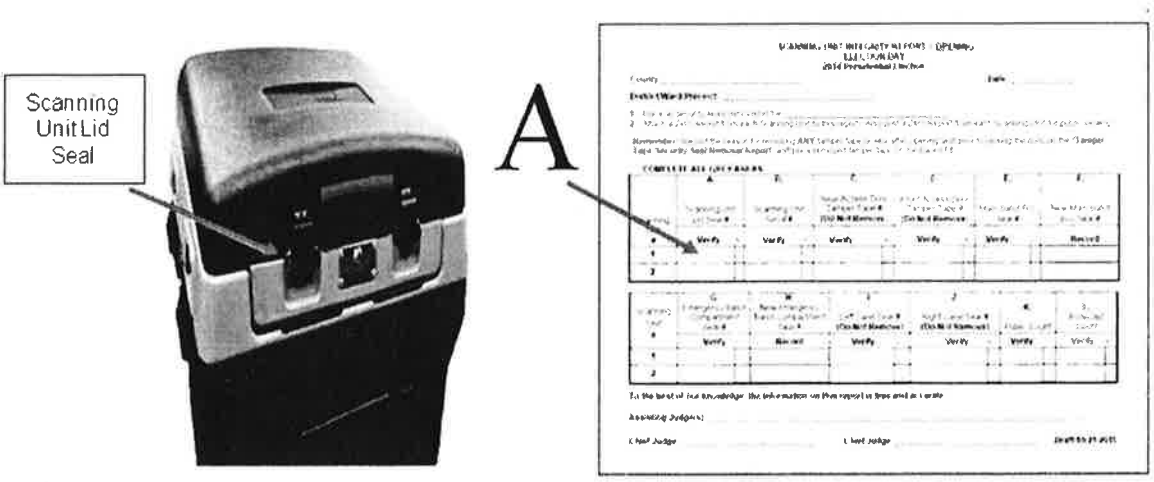
IMPORTANT: Keep the back door of the Scanning Unit open when the Scanning Unit is plugged into an electrical outlet. Failure to do so may result in the unit overheating.

5. Ensure that both lights on the surge protector (red and green) are lit.

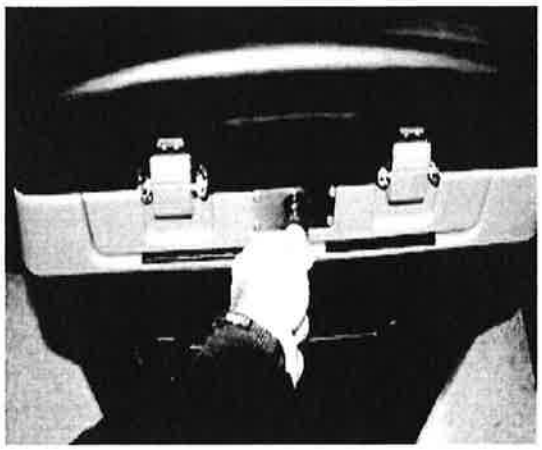


Opening the Polls

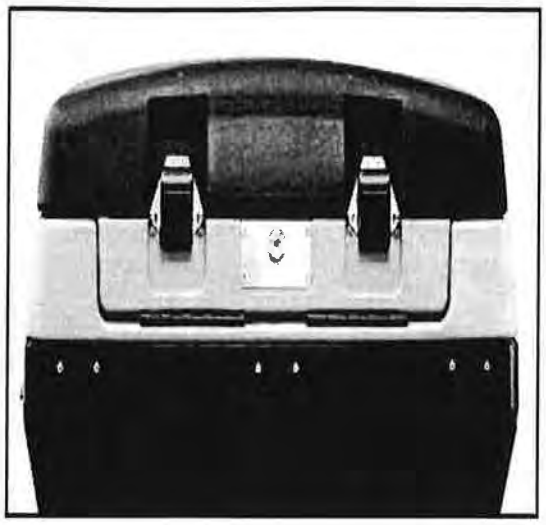
1. **Verify** the security seal number on the Scanning Unit lid (column **A** of the *Scanning Unit Integrity Report – Opening*).



2. Remove the security seal. Use the flat Scanning Unit key to unlock the lid.

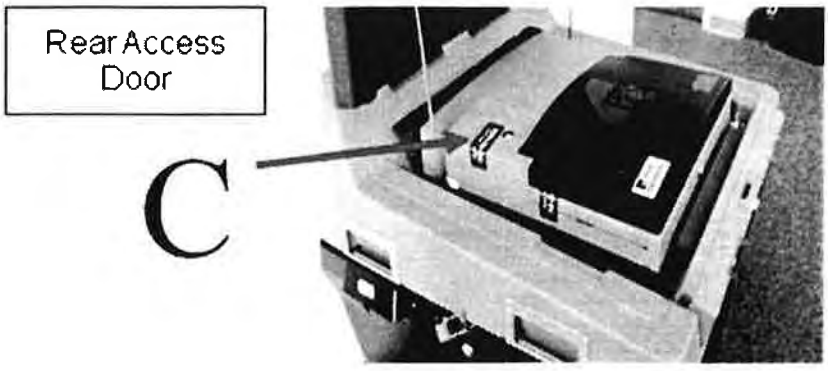


3. Unhook the lid latches. Pull both latches out and flip up. Do not force the lid up. Instead, hold onto the latches as you nudge the lid upward. The hydraulic arms will do the lifting.



4. Verify the serial number on the top of the Scanning Unit (column **B** of the *Scanning Unit Integrity Report - Opening*).

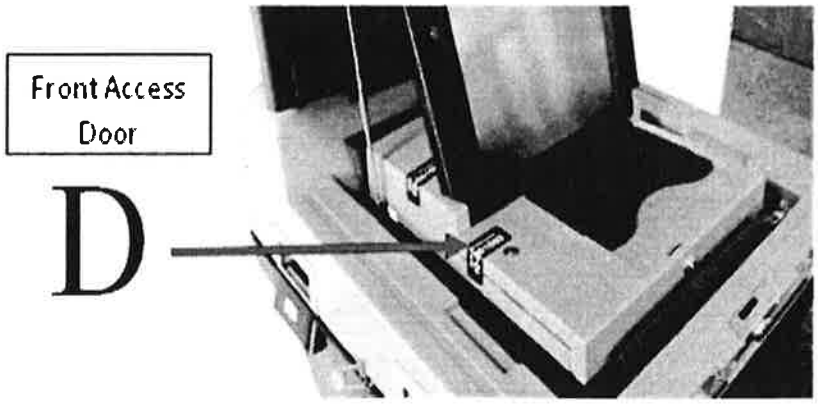
5. **Verify** the tamper tape number on the rear access door (column **C** of the *Scanning Unit Integrity Report – Opening*). **Do NOT remove the tamper tape**.



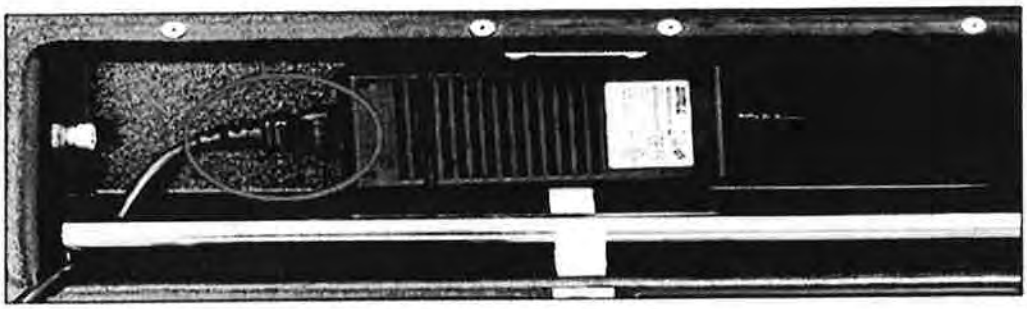
6. Use the round key to unlock and open the Ballot Scanner.

7. Gently lift and raise the screen to the upright position. The Ballot Scanner will turn on by itself. If the Ballot Scanner does not turn on, alert a chief judge.

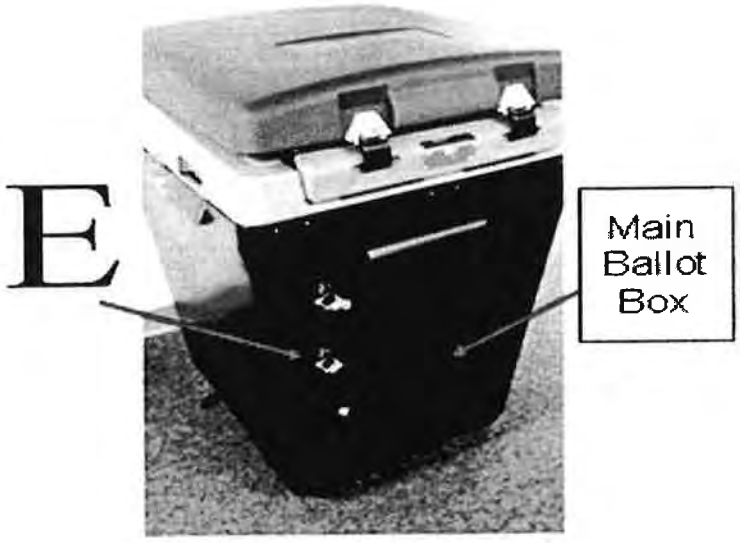
8. **Verify** the tamper tape number on the front access door (column **D** of the *Scanning Unit Integrity Report – Opening*). **Do NOT remove the tamper tape**.



Note: If the scanner does not turn on or if you hear a series of four beeps check the power supply to the Scanning Unit. Make sure power cord is connected firmly in the back of the Scanning Unit and also into the grey surge protector and power outlet. Make sure the power outlet is "live" (i.e., power is coming through the outlet). **If the Ballot Scanner still does not turn on alert a chief judge**.



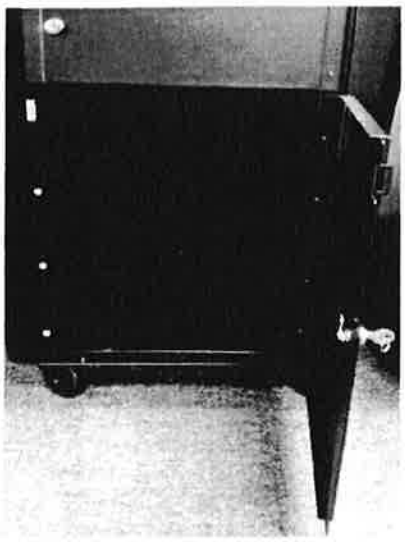
9. **Verify** the number on the security seal on the Main Ballot Box (column **E** of the *Scanning Unit Integrity Report – Opening).*



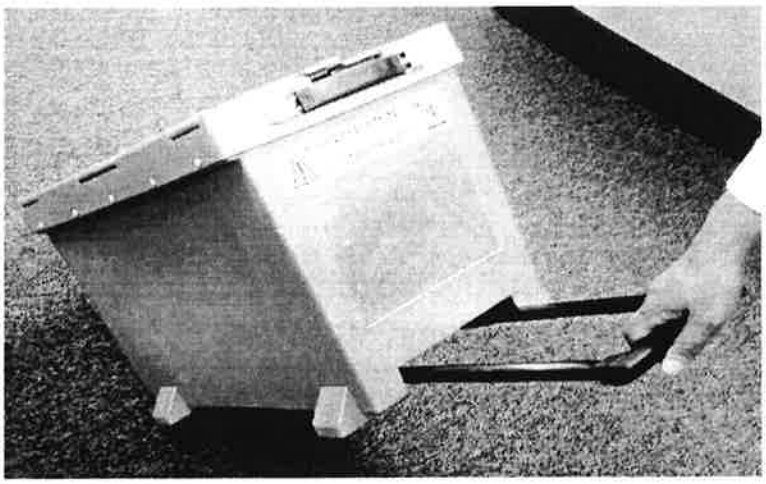
10. **Remove** the security seal on the Main Ballot Box and place it in the Completed Forms Envelope. Use the flat Scanning Unit key to unlock and open the Main Ballot Box door.

11. Use the strap handle to pull the Ballot Transfer Bin out of the Main Ballot Box.

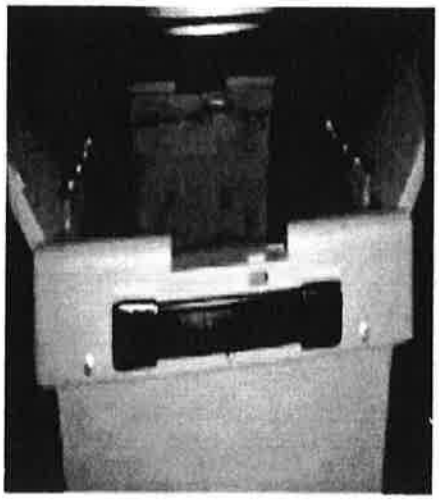
12. You will find the ballots in this Ballot Transfer Bin and possibly the other Transfer Bins that were delivered in the Black Cart. Check inside each for ballots. Look inside the Main Ballot Box to verify that it is empty. If there are any ballots inside the Main Ballot Box, alert a chief judge.



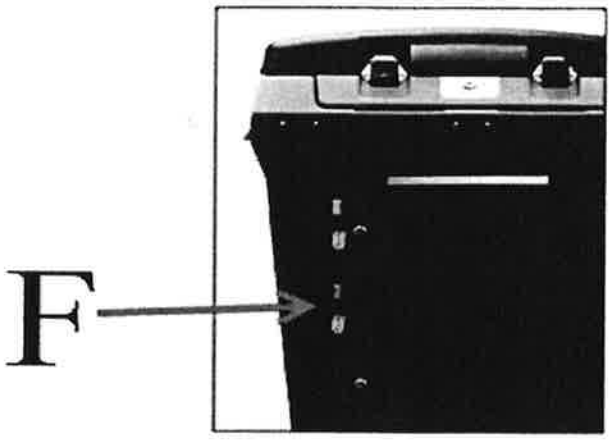
13. Open the lid of the Ballot Transfer Bin and look inside. Extend the roller handle and lift the handle to shift the weight of the Ballot Transfer Bin to the rear wheels. Roll the Ballot Transfer Bin to where its contents will be removed, verified, and counted. Complete the opening portion of the Ballot Certificate. Return the empty Ballot Transfer Bin to the Scanning Unit area and keep the ballots at the Ballot Issuance Table.



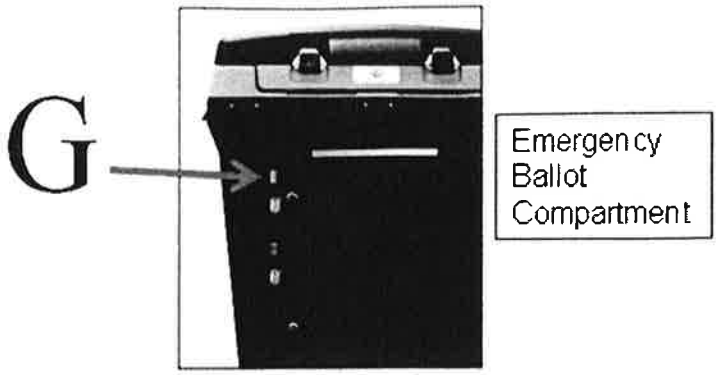
14. Place the empty Ballot Transfer Bin back inside the Main Ballot Box. Ensure that both lids of the Ballot Transfer Bin are open and resting on the sides inside the Main Ballot Box and the strap handle is facing out.



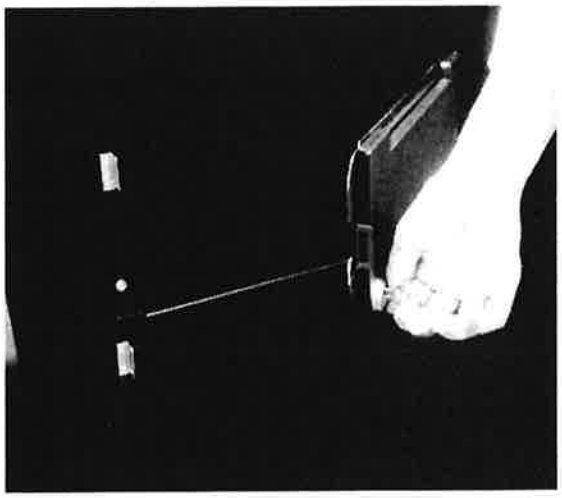
15. Close, lock, and reseal the Main Ballot Box door. **Record** the new seal number in column **F** of the *Scanning Unit Integrity Report - Opening*.



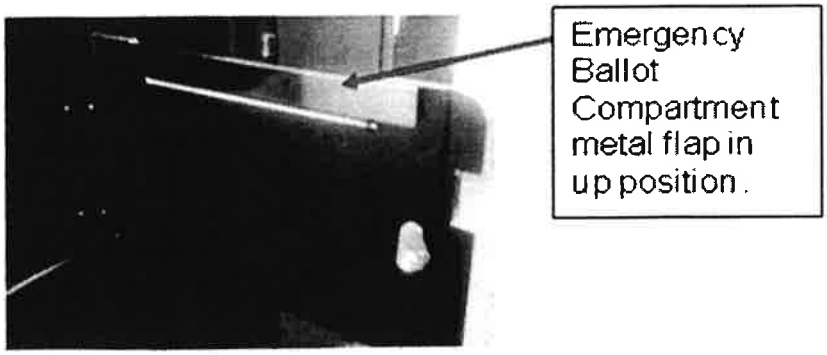
16. **Verify** the number on the security seal on the Emergency Ballot Compartment door (column **G** of the *Scanning Unit Integrity Report – Opening*). Remove the security seal.



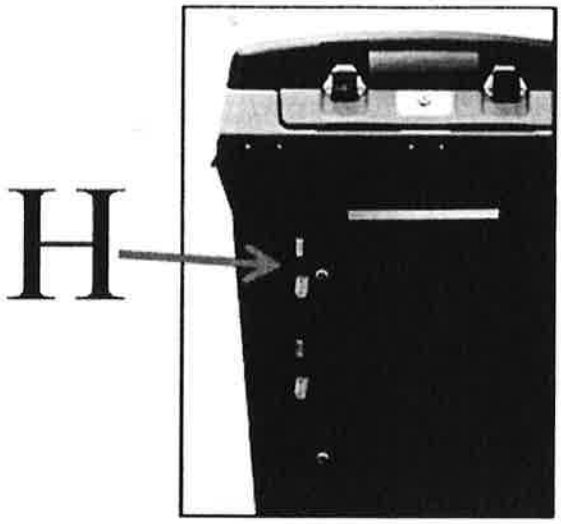
17. Unlock and open the Emergency Ballot Compartment door. Make sure that the compartment is empty. **Beware of sharp edges.** Alert a chief judge if any ballots are found inside the Emergency Ballot Compartment.



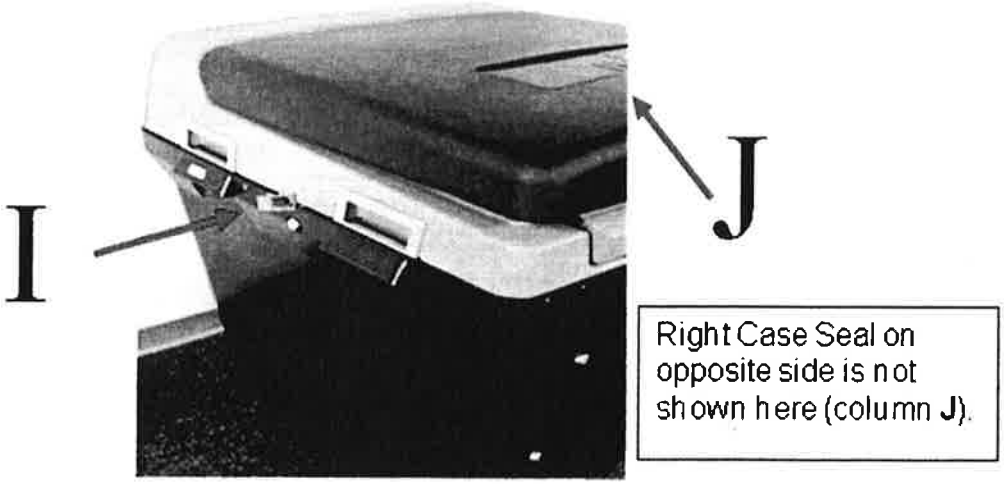
18. Ensure that the metal flap on the Emergency Ballot Compartment door is raised.



19. Close, lock and reseal the Emergency Ballot Compartment door. **Record** the new security seal number in column **H** of the *Scanning Unit Integrity Report - Opening.*

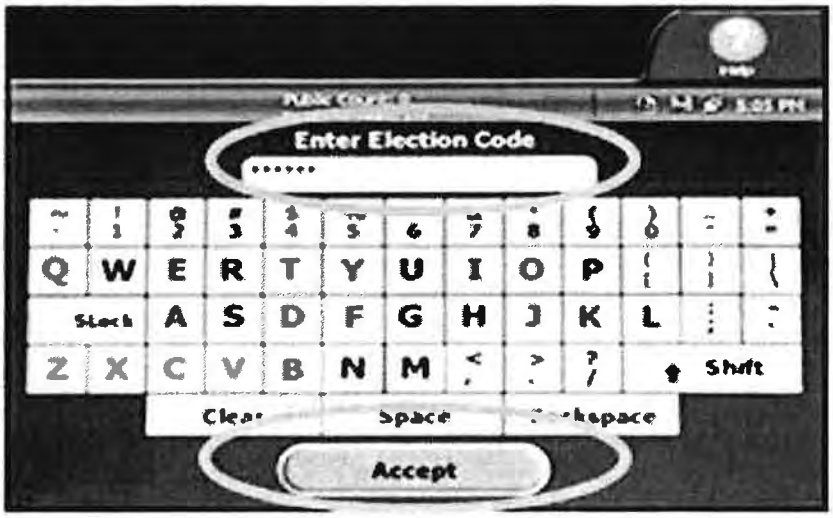


20. **Verify** the left and right side case red seals are intact (columns **I** and **J** of the *Scanning Unit Integrity Report – Opening*). **DO NOT remove the red seals.**



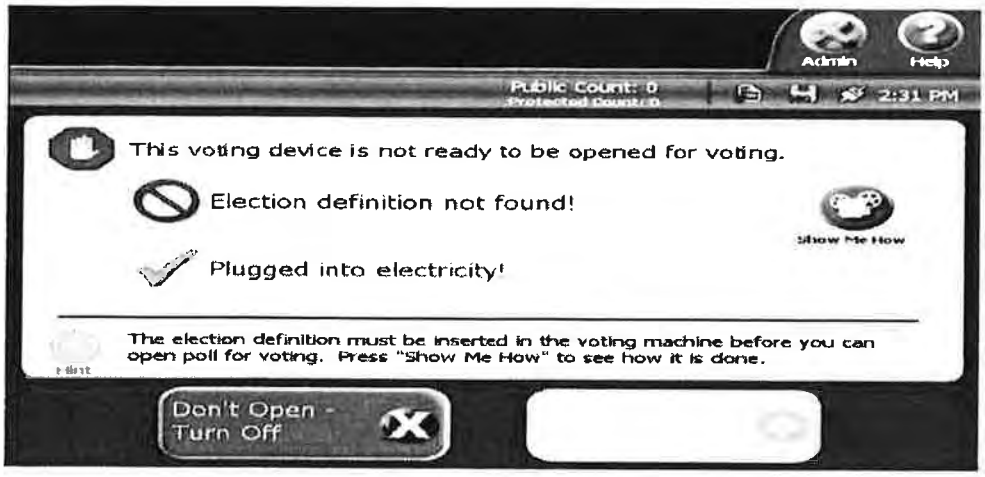
21. Once the Ballot Scanner turns on, **verify** the Public Count number is the same as indicated in column **K** of the *Scanning Unit Integrity Report – Opening*. Also **verify** the Protected Count number is the same as indicated in column **L**.

22. A chief judge enters the Election Code, then touches "**Accept.**"



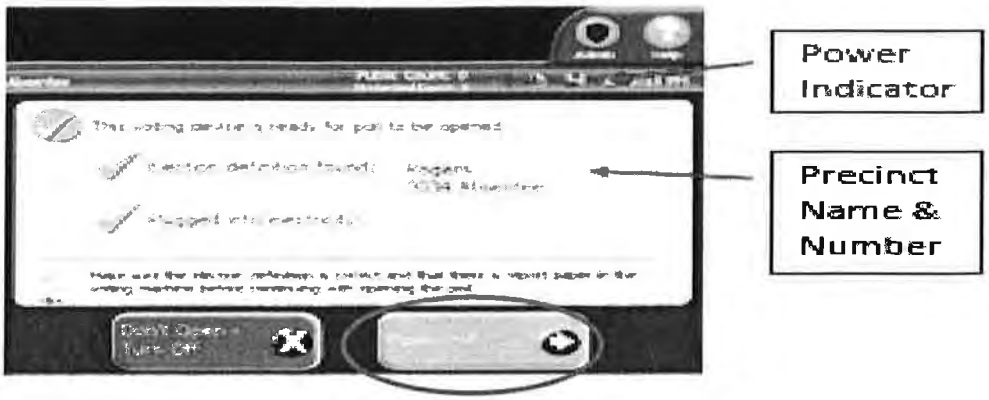
NOTE: The Ballot Scanner performs an internal self-test. This process may take several minutes. **If the following screen appears, or if the Ballot Scanner automatically shuts down, alert a chief judge immediately. Be aware that the unit will automatically shut down after you incorrectly enter the code**

three times. Never turn off the Ballot Scanner or unplug the Scanning Unit unless instructed by the local board of elections.



23. A Configuration Report will automatically print.

24. **Confirm** that the polling place name displayed on the screen is correct and the unit is receiving power. Touch **"Open Poll"** on the screen.



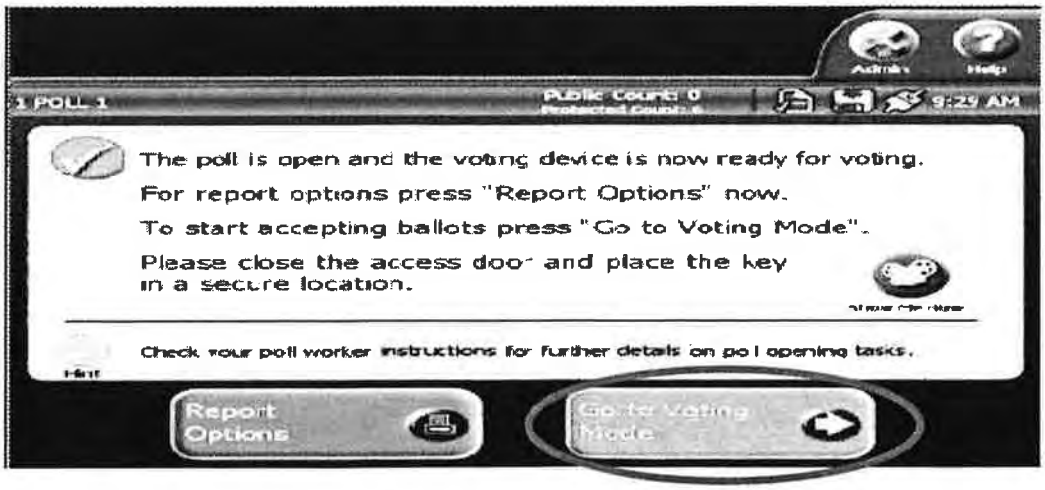
25. Two copies of the "Zero Report" will print. Separate the Zero Reports into two individual reports:

    A. Both chief judges sign both Zero Reports;

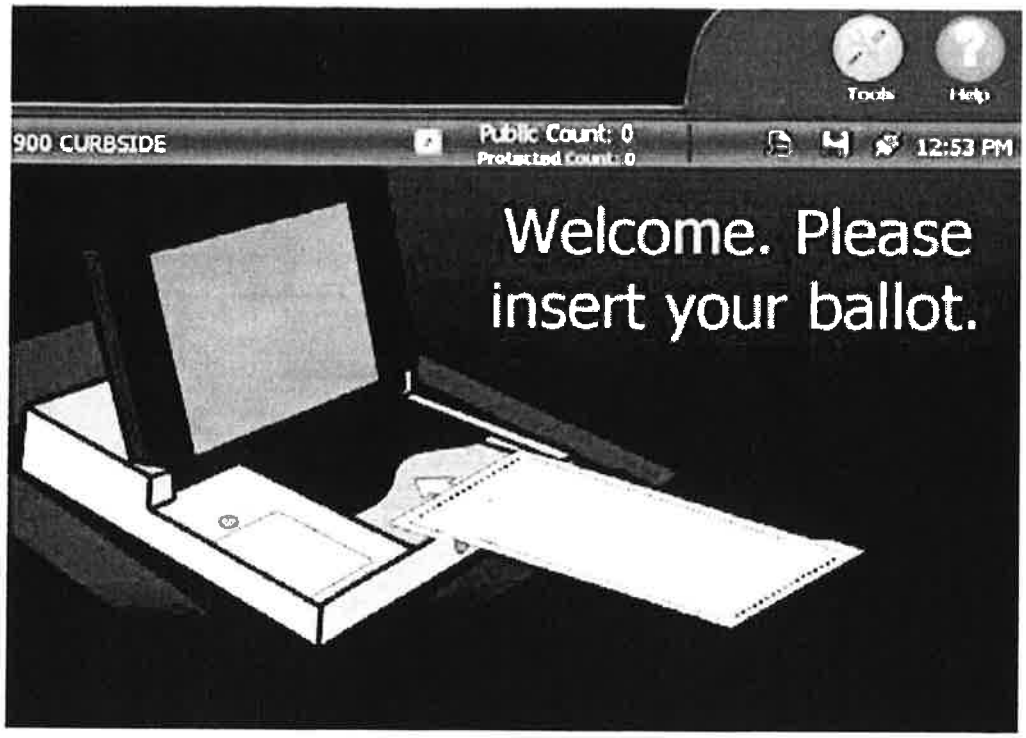
    B. Attach the first copy of the Zero Report (with the Configuration Report still attached) to the *Scanning Unit Integrity Report - Opening*.

    C. Post the second copy of the Zero Report for public viewing.

26. Once the self-test is completed, the following screen appears. Touch **"Go To Voting Mode."**



27. When the Ballot Scanner is ready to receive ballots. The following screen appears.

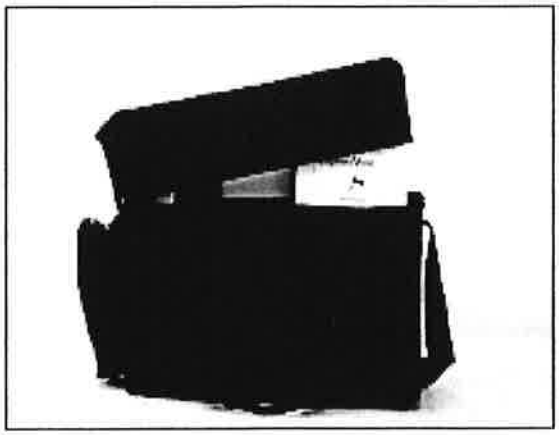

Tools
Help
900 CURBSIDE
Public Count: 0
Protected Count: 0
12:53 PM
Welcome. Please
insert your ballot.

Setting-up the Ballot Marking Device

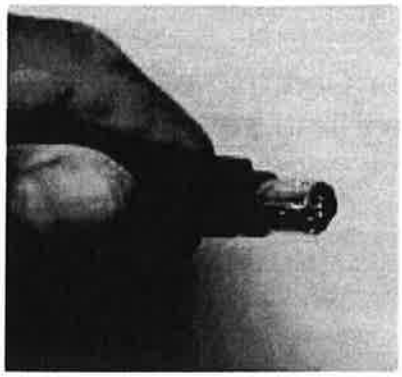
1. Remove the BMD from the Transfer Cart and check the ID tag on the BMD carrying case to ensure that the tag designates the correct polling place.

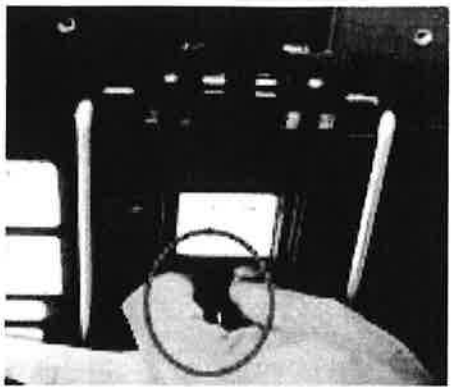
2. Take the BMD in its carrying case to the designated location inside the voting area as shown on the polling place diagram.

3. Remove the BMD, keypad, and headphones from the case. Remove the power cord from the case side pocket.

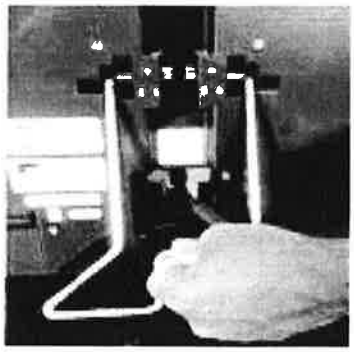


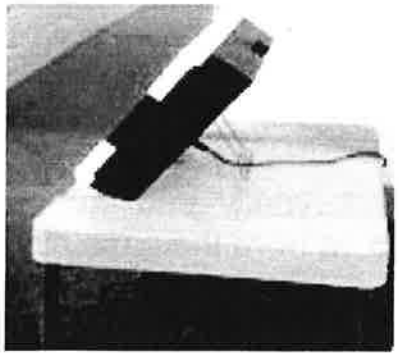
4. Push the small circular plug of the power cord with flat side up into the port on the back of the BMD. The plug will click into place when properly connected. Plug the other end of the power cord into an electrical outlet.



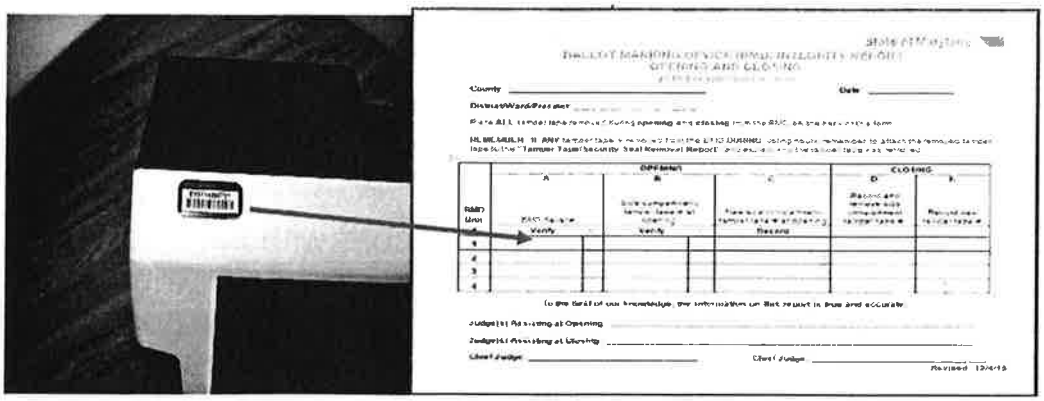


5. Grasp the bottom of the stand on the back of the BMD. Pull out and extend the stand. Rest the BMD on the stand. Position the BMD on the designated table.

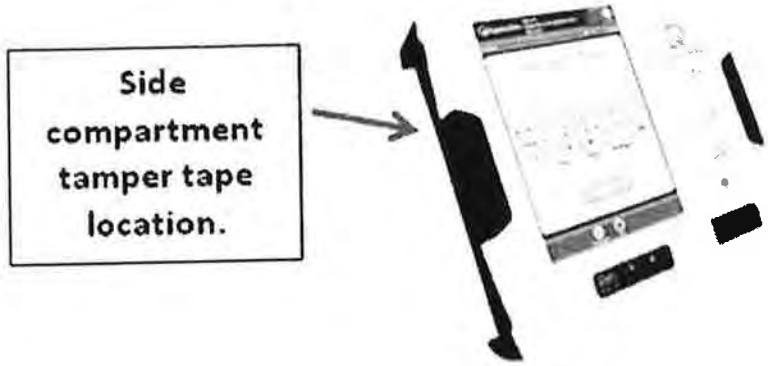




6. Verify the serial number located on the top of the BMD. Confirm by checking the box in column A of the *Ballot Marking Device Integrity Report.*



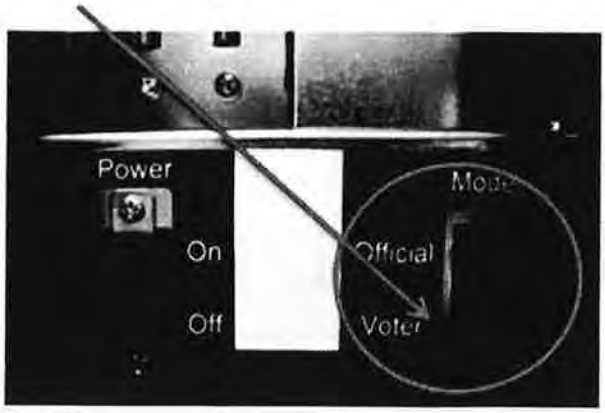
7. Verify the tamper tape number located on the left side compartment door of the BMD. Confirm by checking the box in column B of the *Ballot Marking Device Integrity Report.*



8. Remove the tamper tape and place it on the back of the *Ballot Marking Device Integrity Report.* Use the BMD barrel key to unlock and open the left side compartment door.

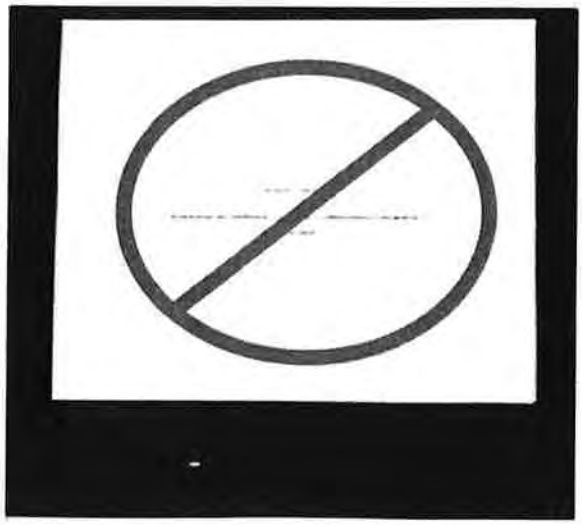
9. Check that the memory stick is installed. If not, immediately notify a chief judge.

10. Check to ensure that the **"Mode"** switch is on **"VOTER."**

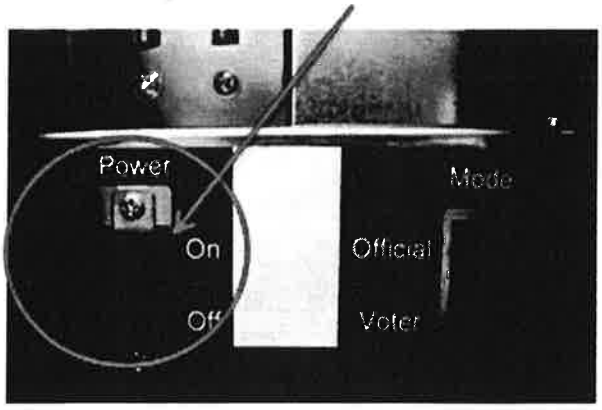


11. Ensure that the keypad is installed before starting up the BMD.

IMPORTANT: **<u>Do not touch the display screen</u> while the BMD is starting up.** Startup is long, about 4 minutes. No reports are printed.

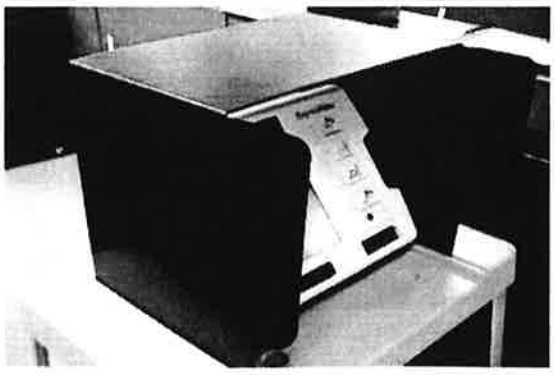


12. Flip the **"Power"** switch to the **"On"** position.



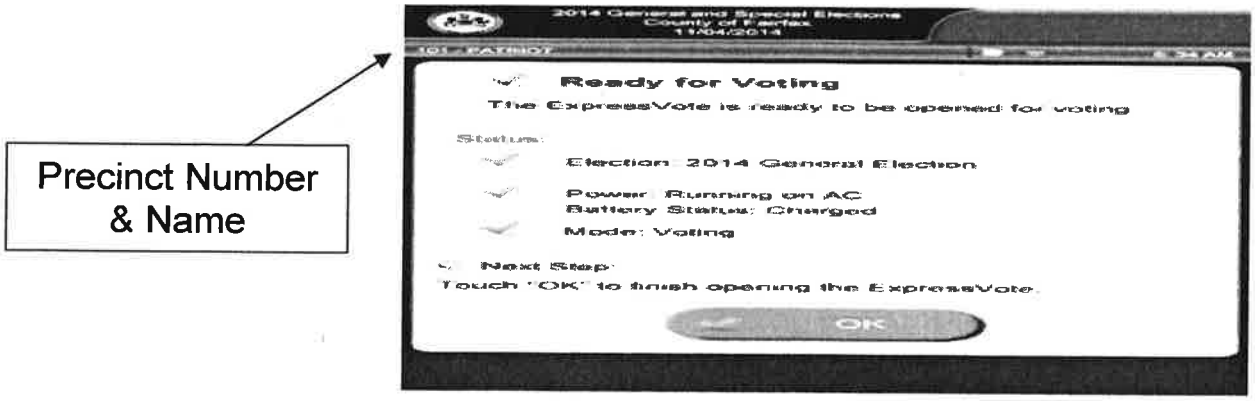
13. Position the keypad cord so it threads through the circular opening at top of the side compartment door. Close and lock the side compartment door. Apply new tamper tape and **record** the new tamper tape number in column **C** of the *Ballot Marking Device Integrity Report*.

14. Install the privacy screen.



15. A Chief Judge enters the Election Code, then touches **Accept**.

16. Verify that the precinct number and name displayed on the screen are correct and the unit is receiving power. Touch **OK**. Contact the local board of elections office immediately if the precinct number and name are incorrect.



17. When the BMD is ready to accept ballots, the following screen appears. Check that the election, county, date and time are correct at the top of the screen.

18. Return the carrying case to the Transfer Cart. Return the key and *Ballot Marking Device Integrity Report* to a chief judge.

Closing the Ballot Marking Device

1. Remove the privacy screen.

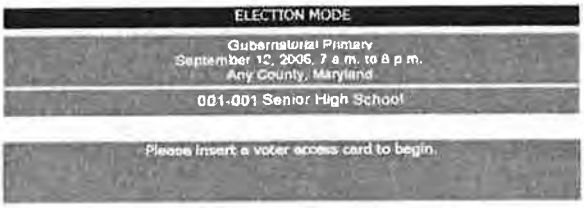
2. Record the side compartment tamper tape number in column D of the closing section of the *Ballot Marking Device Integrity Report.*

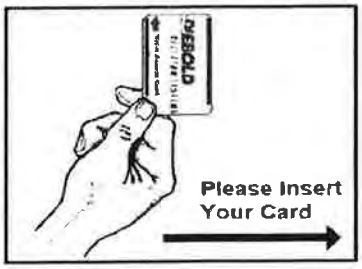
3. Remove the tamper tape from the side compartment. Use the round BMD key to unlock and open the side compartment door.

EXHIBIT C

Ending the Election

1. Record the Ballots Total ("Ballots:" at bottom of screen) and System Total ("Tot:" at bottom of screen) from each voting unit on Page 2 of the *Voting System Integrity Report*.





2. Unsnap the right privacy screen.

3. Verify that the tamper tape currently on the voting unit is intact. **If the word "Void" is visible or there is no tape, call the local board of elections immediately.**

An intact tamper tape

A voided tamper tape

4. Verify that the current tamper tape number matches the number recorded when the tamper tape was attached and record the number on Page 2 of the *Voting System Integrity Report*. **If the number does not match, call the local board of elections immediately.**

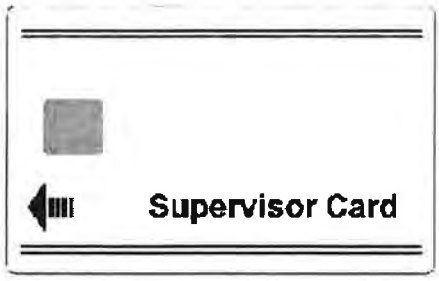
5. Remove the tamper tape and place on the back of Page 2 of the *Voting System Integrity Report*.

6. Unlock the top (printer) compartment.

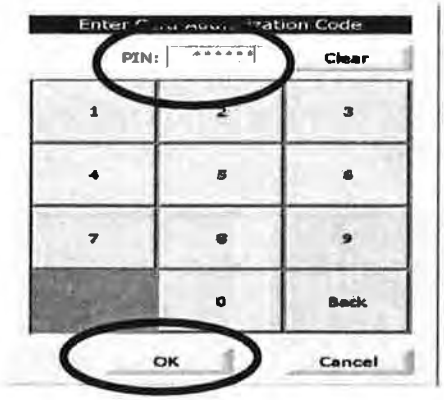
7. To avoid a printer paper jam, either place the printer compartment top under the Zero Report or bend the Zero Report on the outside of the voting unit. **DON'T tear off the Zero Report!**

Don't tear off the Zero Report!

8. Insert the supervisor card into the voting unit where the voter access card is inserted.

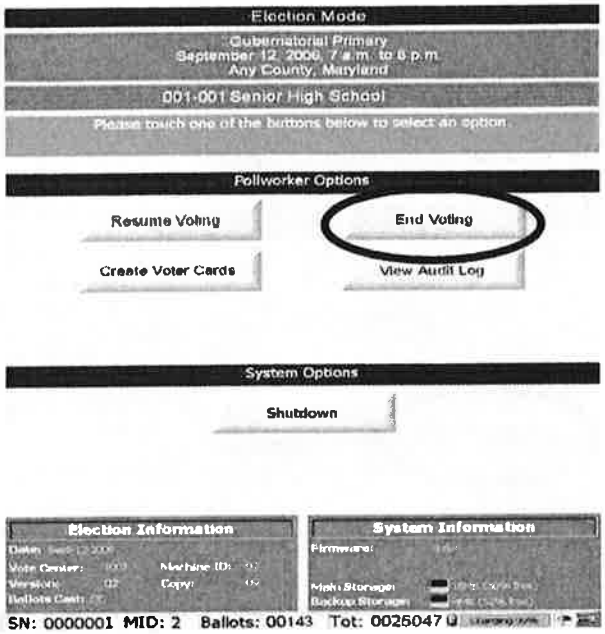


9. Enter the password, and press "OK." The password will be displayed on the screen as all asterisks (*). The supervisor card will then eject, and a "Please remove the access card" message box will show on the screen.

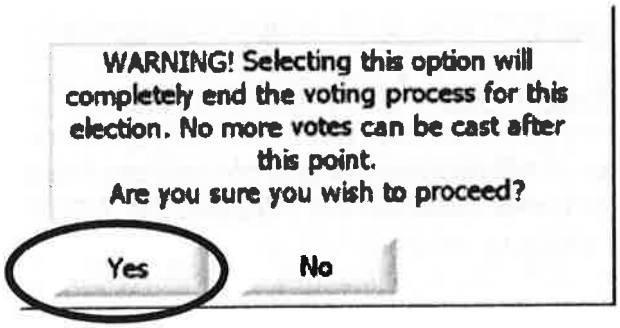


10. Remove the supervisor card and secure it.

11. The "Election Mode" screen will appear. Press the "End Voting" button to close the election and prevent further voting.



12. The "Warning" prompt will appear. Press the "Yes" button to prevent additional voting.



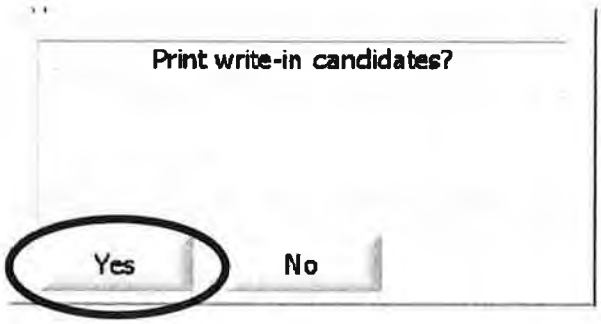
Printing the Totals Reports

1. Print the first Totals Report (which **must** remain attached to the Zero Report already printed):

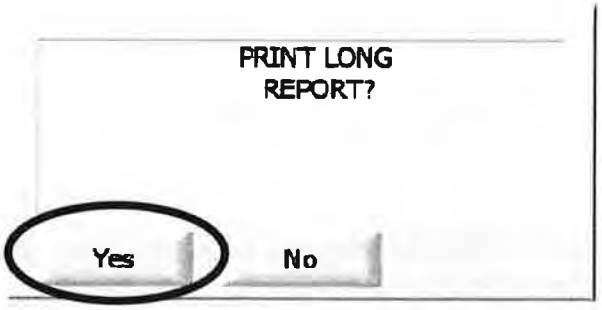
Important

During a primary election, the prompt to print write-in candidates should not appear after pressing the "Print Results" button. If you should get the prompt to "print write-in candidates" during a primary election, select "No" and proceed to step 2 below.

2. **General Election Only:** If write-in votes were cast on the voting unit, the "Print write-in candidates?" prompt will appear. Press "Yes." (If there were no write-in votes cast, the prompt will not appear. Proceed to step 3.)



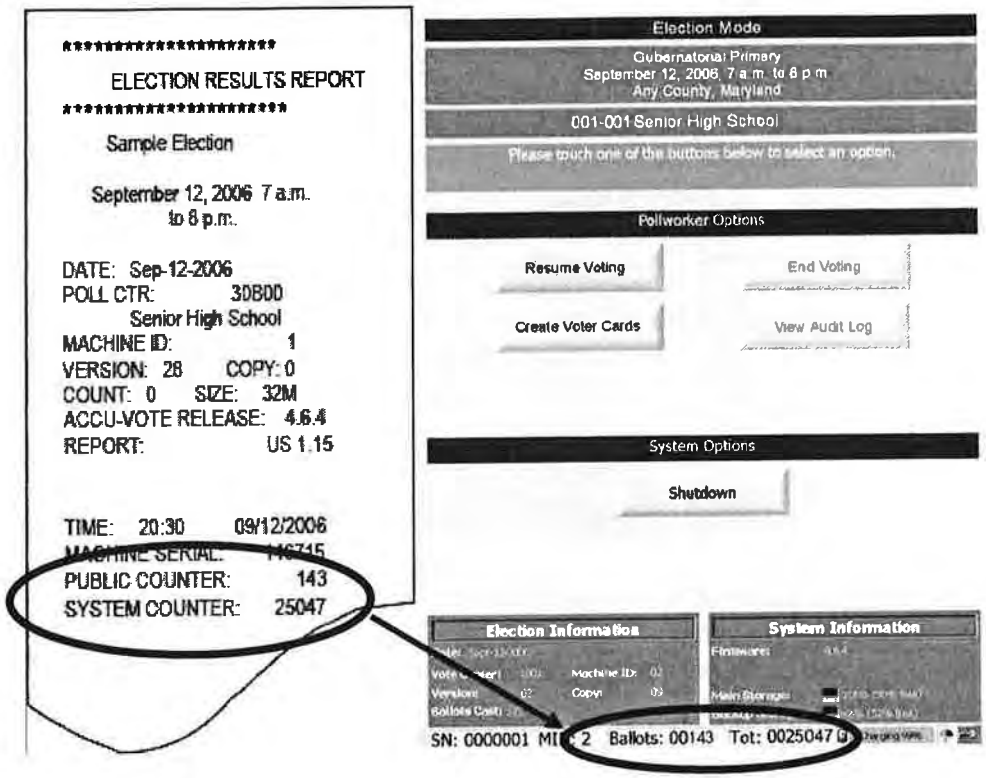
3. The "Print Long Report?" prompt will appear. Press the "Yes" button.



4. The Totals Report will print at the end of the Zero Report. **DO NOT** separate the zero report from the 1st copy of the Totals Report. Tear off the reports **without** separating them.

⚠ **DON'T** separate the Zero Report and the 1st copy of the Totals Report!

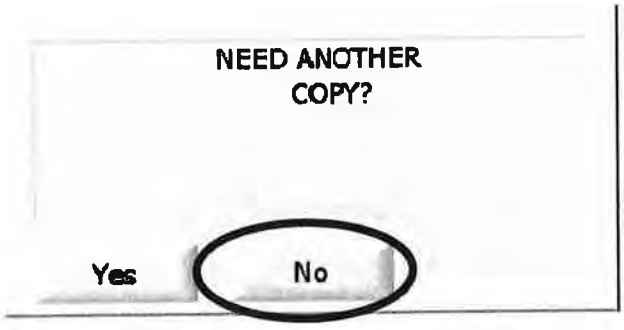
Note: If "Public Counter" on the Totals Report is **NOT** the same as "Ballots" on the touchscreen or if "System Counter" is **NOT** the same as "Tot" on the touchscreen, call the local board of elections **immediately**.



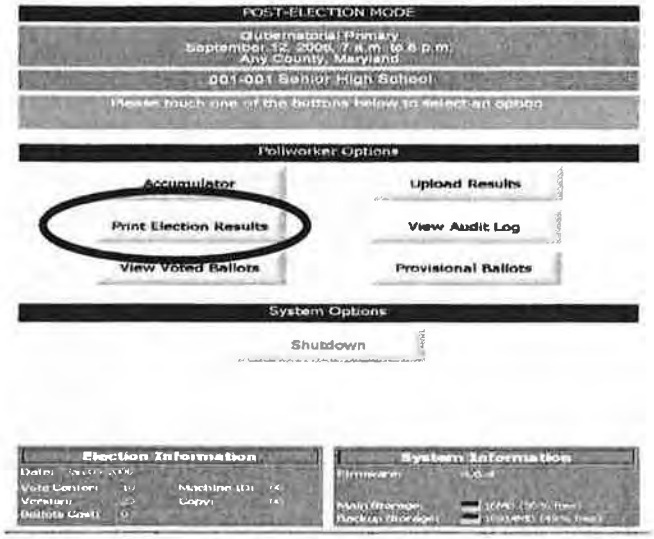
5. **Two election judges** must sign at the bottom of the Zero/Totals Report.

6. Secure the Zero/Totals Report in the red bank bag for transport. These reports will be returned to the local board of elections with the memory cards. **Do not post the Zero/Totals Report.**

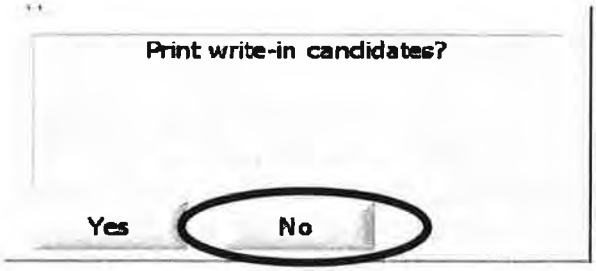
7. The "Need Another Copy?" prompt will appear. Press "No."



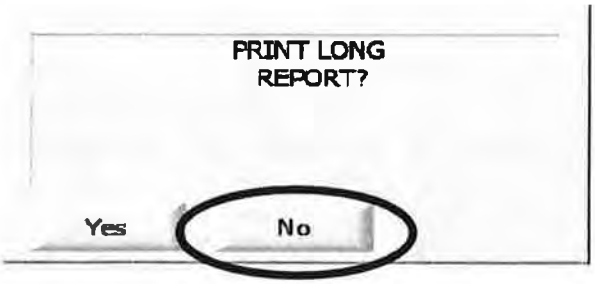
8. The "Post Election Mode" screen will appear. Press the "Print Election Results" button.



9. **General Election only:** If write-in votes were cast on the voting unit, the "Print write-in candidates?" prompt will appear. Press "No." (If there were no write-in votes cast on the voting unit, the prompt will not appear.)



10. The "Print Long Report?" prompt will appear. Press the "No" button.

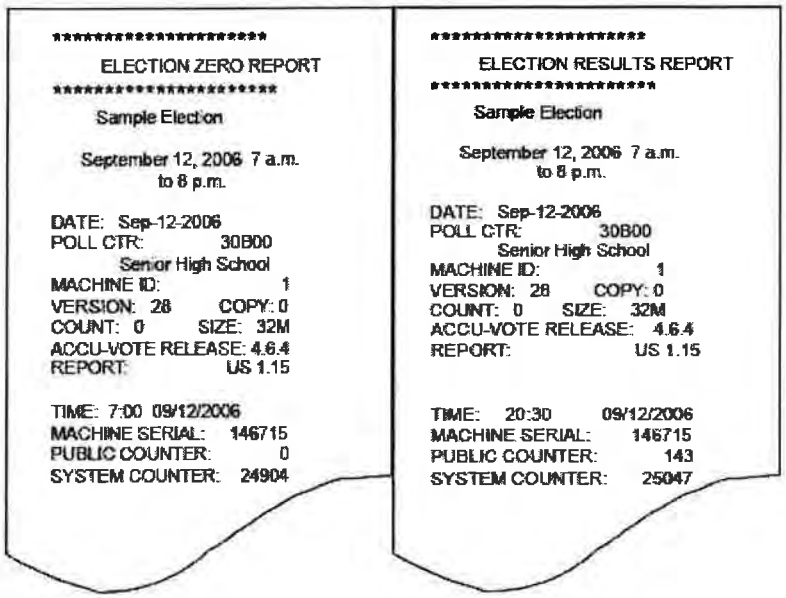


11. The 2nd Totals Report will print. Tear off the 2nd Totals Report.

⚠ The 2nd copy of the Totals Report is **NOT** a long report.

12. **Two election judges** must sign the 2nd Totals Report.

13. Post the 2nd Totals Report beside the posted Zero Report.



****
ELECTION ZERO REPORT
****
Sample Election

September 12, 2006 7 a.m.
to 8 p.m.

DATE: Sep-12-2006
POLL CTR: 30B00
Senior High School
MACHINE ID: 1
VERSION: 28 COPY: 0
COUNT: 0 SIZE: 32M
ACCU-VOTE RELEASE: 4.6.4
REPORT: US 1.15

TIME: 7:00 09/12/2006
MACHINE SERIAL: 146715
PUBLIC COUNTER: 0
SYSTEM COUNTER: 24904

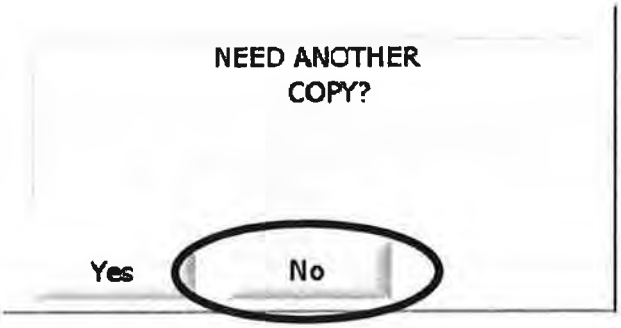
****
ELECTION RESULTS REPORT
****
Sample Election

September 12, 2006 7 a.m.
to 8 p.m.

DATE: Sep-12-2006
POLL CTR: 30B00
Senior High School
MACHINE ID: 1
VERSION: 28 COPY: 0
COUNT: 0 SIZE: 32M
ACCU-VOTE RELEASE: 4.6.4
REPORT: US 1.15

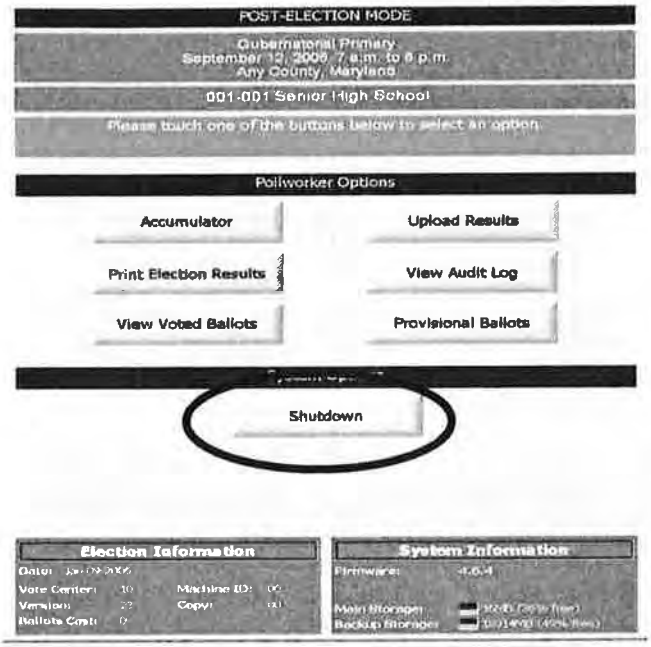
TIME: 20:30 09/12/2006
MACHINE SERIAL: 146715
PUBLIC COUNTER: 143
SYSTEM COUNTER: 25047

14. The "Need another copy?" prompt will appear. Press the "No" button.



Note: If results are to be accumulated and transmitted, <u>do NOT shut down or remove the memory card from the accumulator unit</u>. Proceed to Appendix 4, "Accumulating and Transmitting Results" for further instructions.

15. At the "Post-Election Mode" screen, press the "Shutdown" button on the screen.

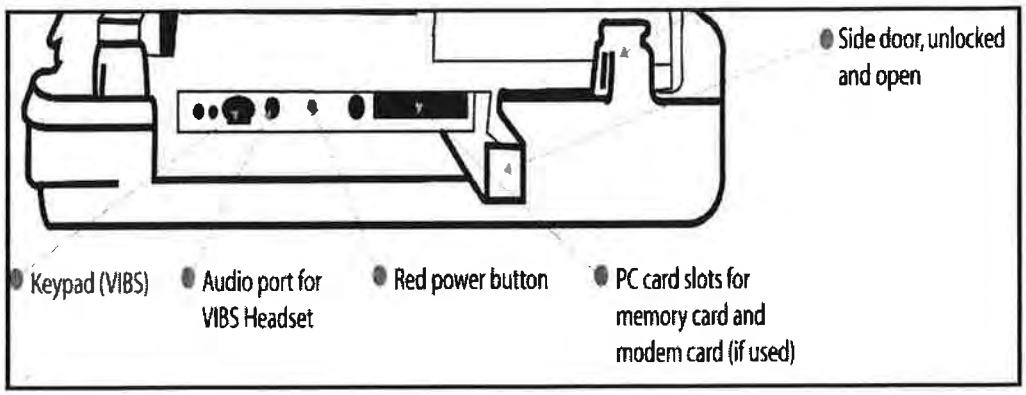


16. A message will appear, "Are you sure you want to shut down the voting terminal?" Press "Yes."

⚠ **DON'T** shut down the **accumulator unit** if accumulating results.

17. Another message will appear, "System Shutdown OK to turn power off." Press the red power button in the side compartment to shut down the voting unit.

18. Press the black button to the left of the PC card slot to remove the memory card from the side compartment.



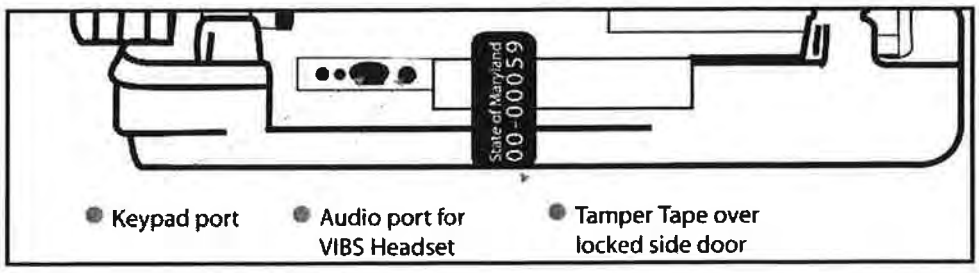
19. Record (or verify) the memory card's serial number (found on the back of the memory card above the barcode) on Page 2 of the *Voting System Integrity Report*.

20. Close and lock the side compartment door.

21. Locate the new tamper tape in the Chief Judge's Case.

22. Record the new tamper tape number on Page 2 of the *Voting System Integrity Report*.

23. Put the tamper tape over the keyhole for the side compartment. The tamper tape must extend above and below the door to the side compartment. See the illustration below for the proper positioning of the tamper tape.



24. Pack up the memory cards. Secure them in the red bank bag for transport.

Taking Down the Voting Units

Once the tamper tape has been placed over the locked side compartment door, the voting unit judges can take down the voting unit.

1. Verify that the top printer compartment is locked and tamper tape has been placed over the locked side compartment door.

2. Unplug the power cord and place in metal box attached to carts.

3. Disconnect headphones and keypad from the accessible voting unit and return to supply bag (purple bag with red tag).

4. Lower screen to the flat position by pressing the black button on the top of the screen and folding the adjustable metal bar. Make sure that the screen is locked in place.

5. Fold the right privacy screen into the voting unit lid. Repeat with left screen. Do not force screens.

6. Close the top of the case, and make sure it locks into place.

7. Make sure the voting unit tag or label is still attached to the voting unit. If there is no tag attached, notify the Chief Judges.

8. Seal the voting unit case. (Seals are found in the Chief Judges' Case.)

9. Record (or verify) the seal number on Page 2 of the *Voting System Integrity Report*.

10. Using two people, place the voting unit upside down on the floor or table.

11. Open the black securing latch in the middle of each leg.

12. Push in the silver button to lower the leg, and close the black securing latch. Repeat for each leg.

13. Open the black latch at the base of the legs, and fold legs into case. If legs are not flat, unfold and fold other set of legs first. **Don't** force!

14. Close the black latches at the base of the legs.

15. Place the voting unit on its side so that you can pull the retractable handle up.

16. Repeat steps 1-15 for each voting unit.

Packing the Voting Units

Pack all voting units on the blue cart that was used to deliver them.

Remember to pack the voting units side by side and not in a tower.

Make sure you thread the wire through the handles to secure the units on the cart. Then loop the wire through the two metal brackets on the bottom of the cart and secure the wire to it. This ensures that the voting units do not slide around during transport.

Place all the electrical cords in the metal box attached to the carts.

Remember to take the headphones and keypad off the zero machine and store them in the supply bag.

Put cart and all supplies in the pre-determined secured location for pick-up (this is the same place you found the units).

EXHIBIT D

Closing the Polls

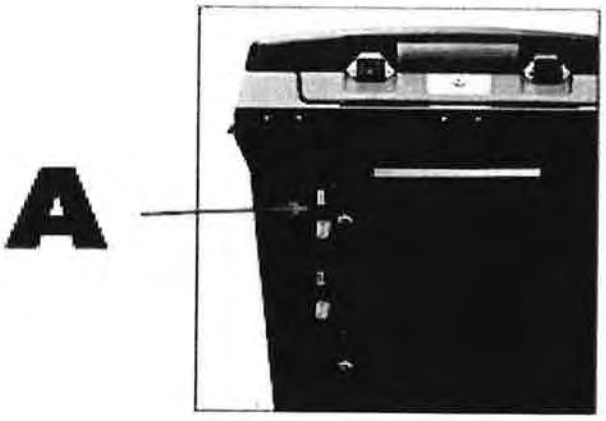
At the direction of the Chief Judges, the following procedures are to be completed when the last eligible voter in the polling place has completed the voting process.

The following procedures must be done as a bipartisan team either by Chief Judges or by Voting Judges under the direct supervision of Chief Judges:

The Emergency Ballot Compartment is used to store voted ballots if Scanning Unit malfunctions during voting hours.

IMPORTANT: Ballots that are placed into the Emergency Ballot Compartment shall not be removed until the last voter in line has voted at the end of the day. A bipartisan team of two election judges shall remove the ballots from the compartment and insert them into the scanner.

1. **Record** the security seal number of the Emergency Ballot Compartment in column **A** of the *Scanning Unit Integrity Report - Closing*.

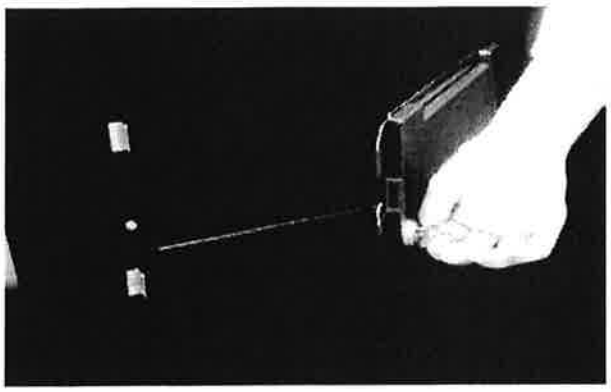


A. Remove the security seal on the Emergency Ballot Compartment and place it in the Completed Forms Envelope.

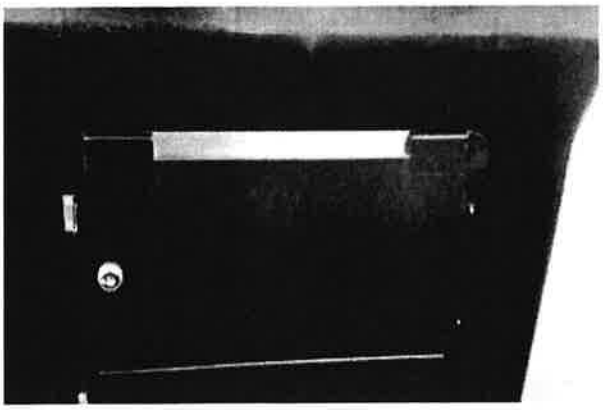
B. Use the flat Scanning Unit key to unlock the Emergency Ballot Compartment.

2. Open the Emergency Ballot Compartment door. Confirm that the Emergency Ballot Compartment is empty. **Beware of sharp edges.**

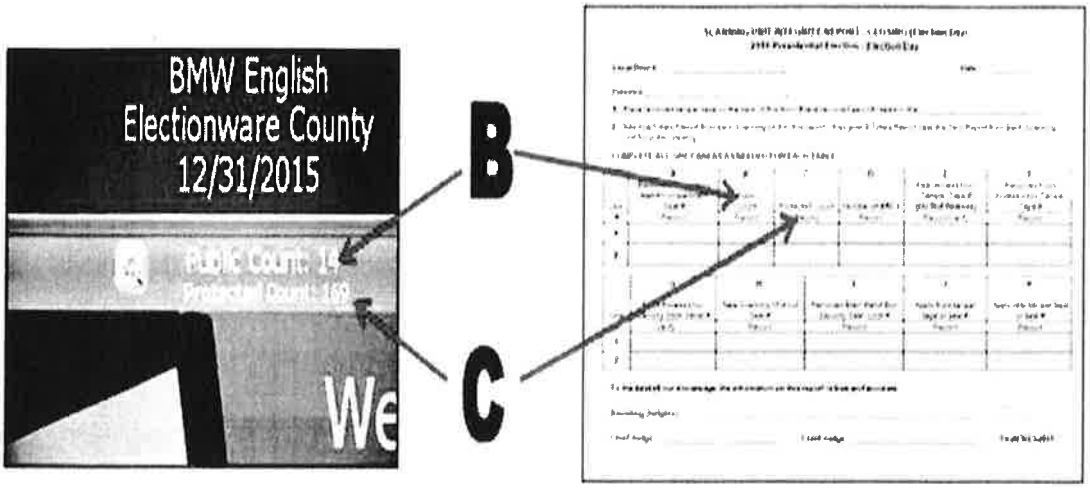
   IMPORTANT: Alert a chief judge if any ballots are found inside the Emergency Ballot Compartment.



3. Close and lock the Emergency Ballot Compartment. A new security seal does not have to be applied.

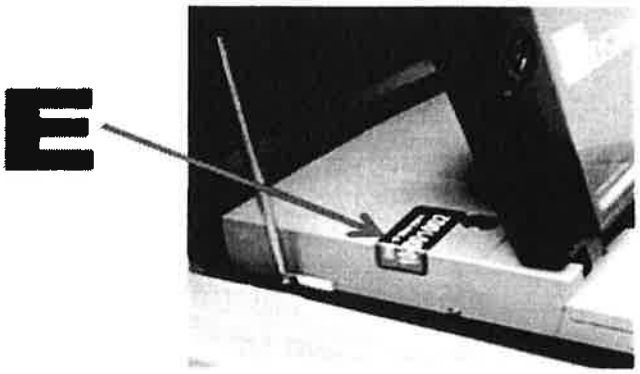


4. Record the Public Count and Protected Count (final vote count) numbers in columns **B** and **C** on the *Scanning Unit Integrity Report - Closing*.

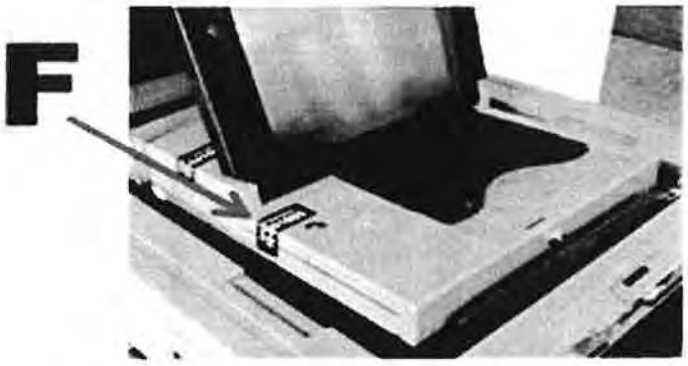


5. Count the number of VACs from the Scanning Unit VAC Envelope. Record the number of VACs in column **D** on the *Scanning Unit Integrity Report - Closing*. Place the VACs back into the VAC Envelope and give the envelope to the chief judges.

6. Record (or verify) the Rear Access Door tamper tape number in column **E** of the *Scanning Unit Integrity Report - Closing*. **DO NOT remove the tamper tape.**

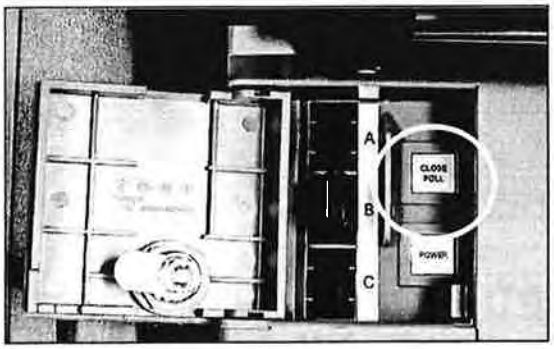


7. Remove the tamper tape securing the Front Access Door, and record the tamper tape number in column **F** of the *Scanning Unit Integrity Report - Closing*. Place the removed tamper tape on the back of the report.

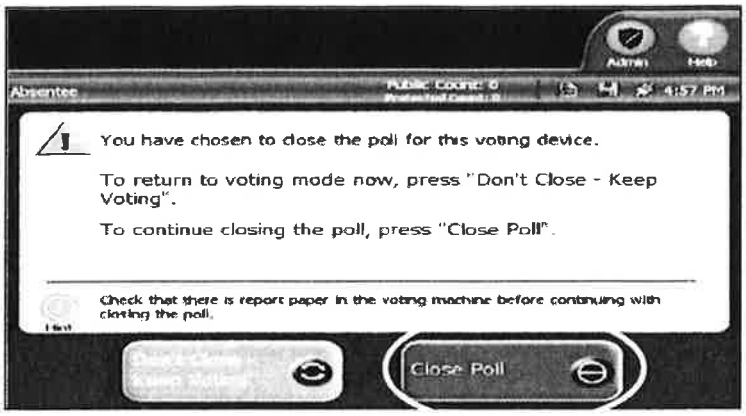


8. Use the round key to unlock and open the front access door.

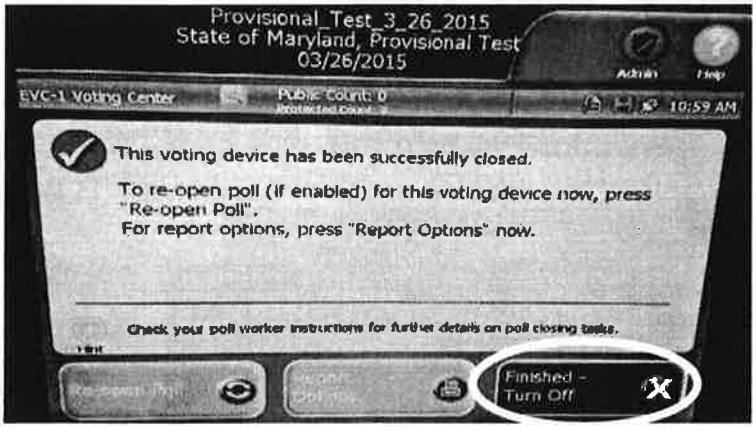
9. Push and hold down the **"Close Poll"** button for a second or two and release. The button will turn red.



10. The Ballot Scanner display reads "You have chosen to close the poll for this voting device." Touch **"Close Poll"** on the display screen. Two copies of the "Results Report" will print.

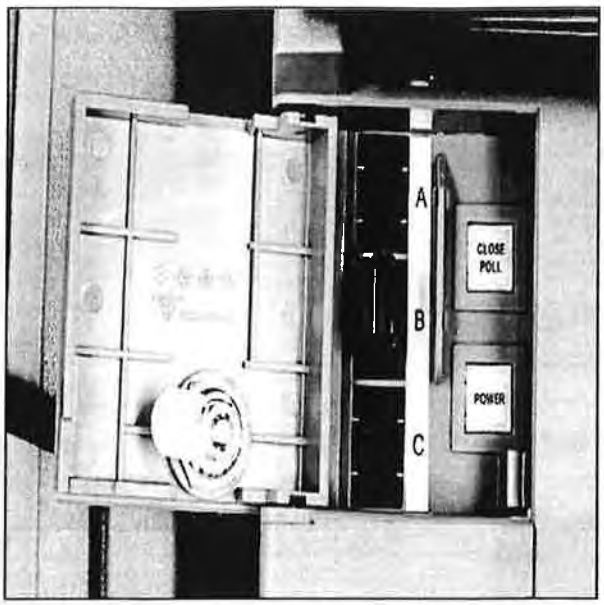


11. After the "Results Reports" have finished printing, the display screen reads "This voting device has been successfully closed." Touch **"Finished – Turn Off."** Scanning Unit powers off and **WAIT!**

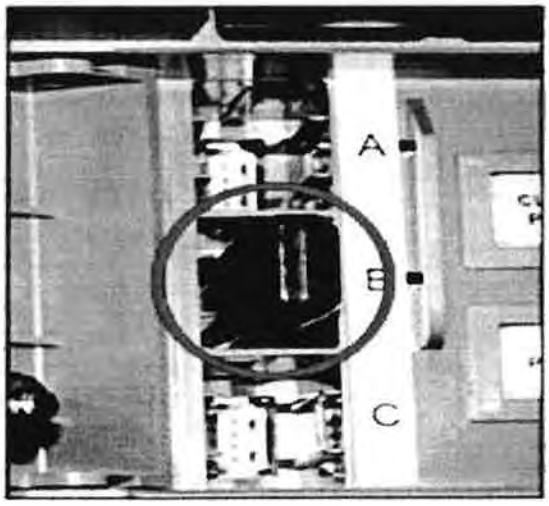


12. **IMPORTANT: Allow all lights in the front access compartment and on the display screen to go completely dark. THIS PROCESS CAN TAKE SEVERAL MINUTES TO COMPLETE.**

    Unplug the Scanning Unit from the power outlet.



13. **After the lights have gone dark**, and after the Scanning Unit has been unplugged from the power outlet, grasp and gently pull the Memory Stick straight out to remove it from the front access door compartment.

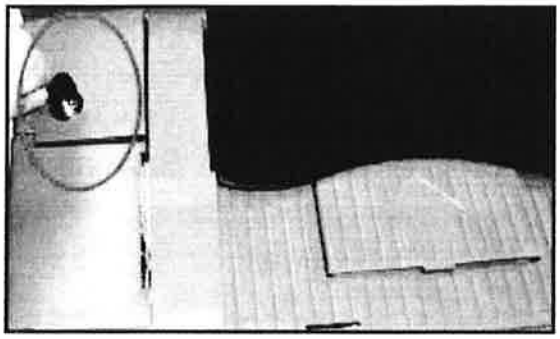


14. Verify the Memory Stick serial number in column **G** of the Scanning Unit Integrity Report- Closing. **Immediately give the Memory Stick to a Chief Judge who will secure it in the Red**

Bank Bag for transport to the local board of elections office.

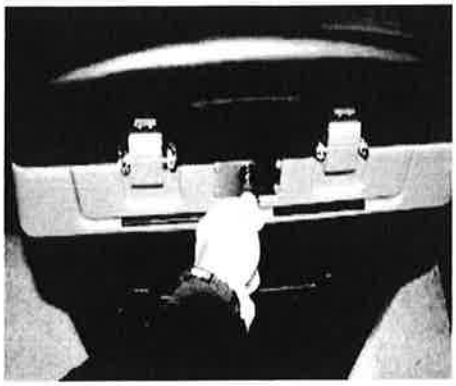
G

15. Close and lock the front access door. Do not apply new tamper tape.



16. Gently lower the display screen and lock the screen into place.

17. Carefully lower the lid while holding the latches and lock the lid. Open rear access door to remove the second memory stick from and place in Clear Bank Bag for technicians to transport.



18. Attach a new security seal to the Scanning Unit lid. Record the new seal number in column **H** of the *Scanning Unit Integrity Report – Closing*.

H

19. Separate the "Results Reports" into two individual reports:

    A. Both chief judges sign both Results Reports;

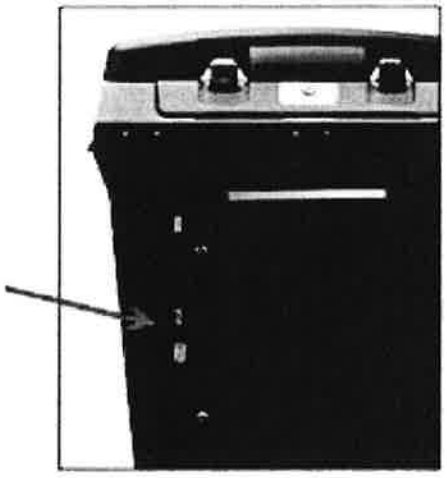
    B. Attach the first copy of the Results Report to the Scanning Unit *Integrity Report - Closing*.

C. Post the second Results Report next to the morning's Zero Report for public viewing.

20. **Record** the security seal number of the Main Ballot Box in column **I** of the *Scanning Unit Integrity Report - Closing*.

A. Remove the security seal on the Main Ballot Box and place it in the Completed Forms Envelope.

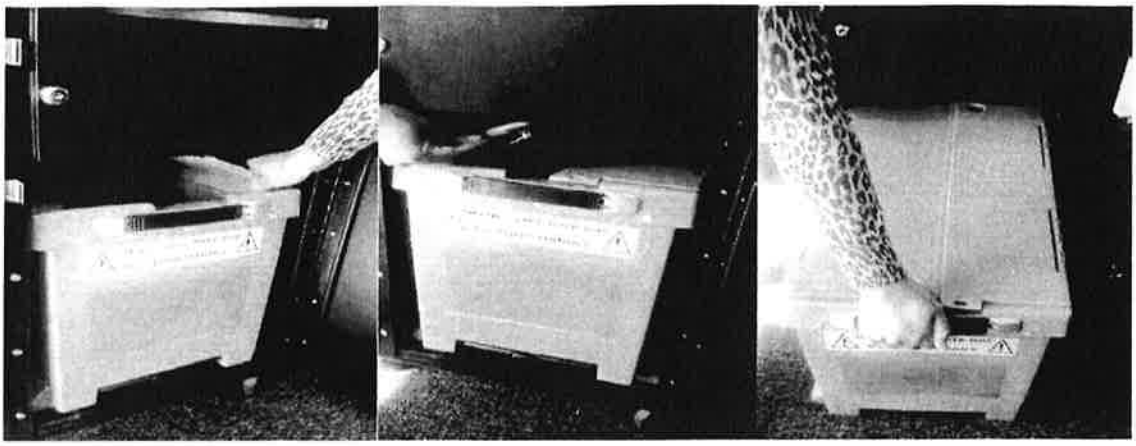
B. Use the Scanning Unit key to unlock the Main Ballot Box.



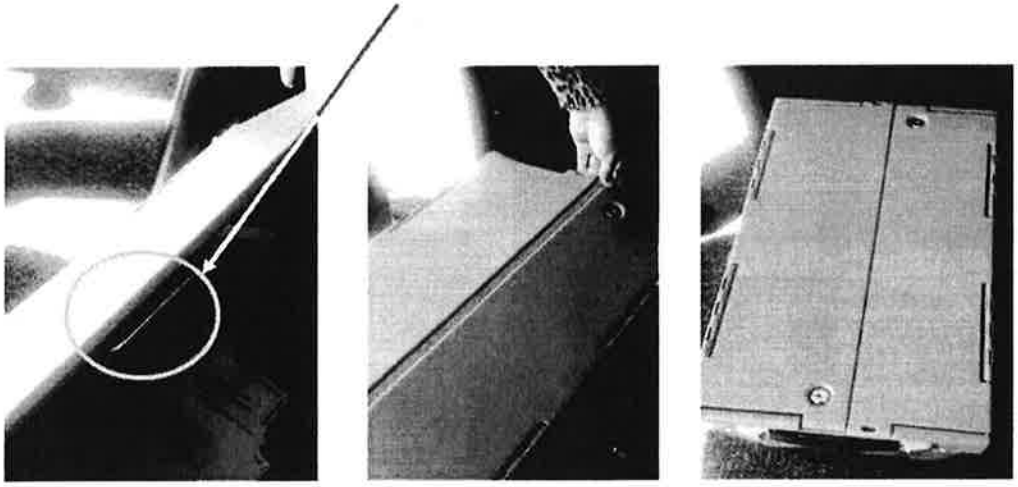
21. Reach inside the Main Ballot Box to close the lid loosely on the Ballot Transfer Bin. Use the strap handle to remove the Ballot Transfer Bin.

A. Check that all ballots are inside the Ballot Transfer Bin.

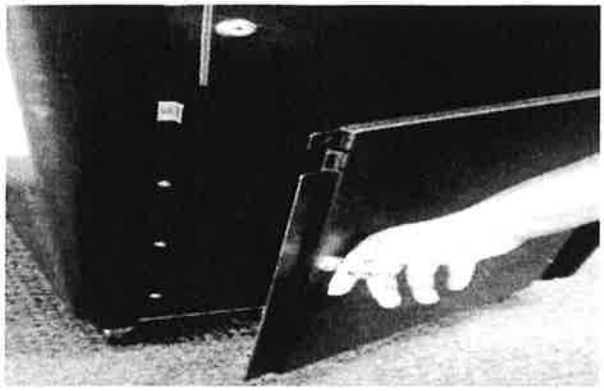
B. Check inside the Main Ballot Box for any loose ballots. Place any loose ballots found inside the Main Ballot Box into the Ballot Transfer Bin.



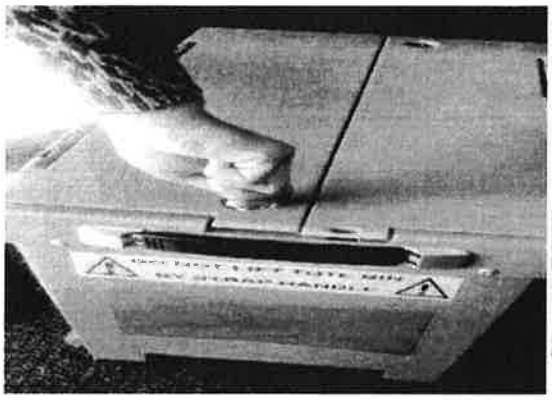
22. Tightly close the lid on the Ballot Transfer Bin. Note that the lid has a "tongue-in-groove" fit. Make sure the right side of the lid is inserted into the metal bracket in the middle of the left side of the lid. The lid sits flat when closed properly.

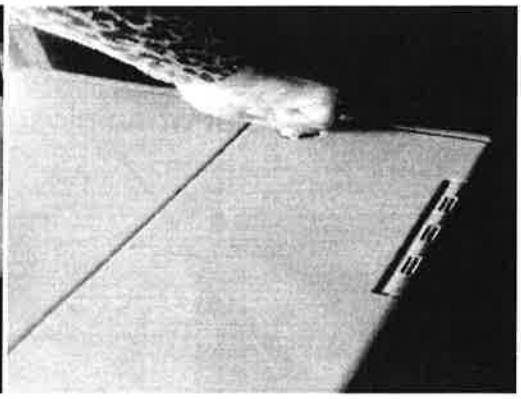


23. Close and use the flat key to lock the Main Ballot Box. A new security seal does not have to be applied.



24. Use the flat key to lock both locks on the Ballot Transfer Bin.



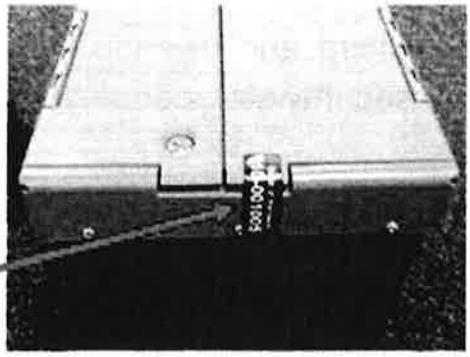


25. Apply green seals on the front and rear of the Ballot Transfer Bin lid. Record the seal numbers in columns **J** and **K** of the *Scanning Unit Integrity Report - Closing.*

Front

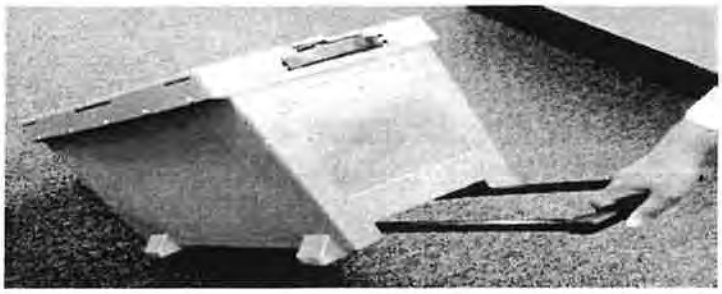
J

K



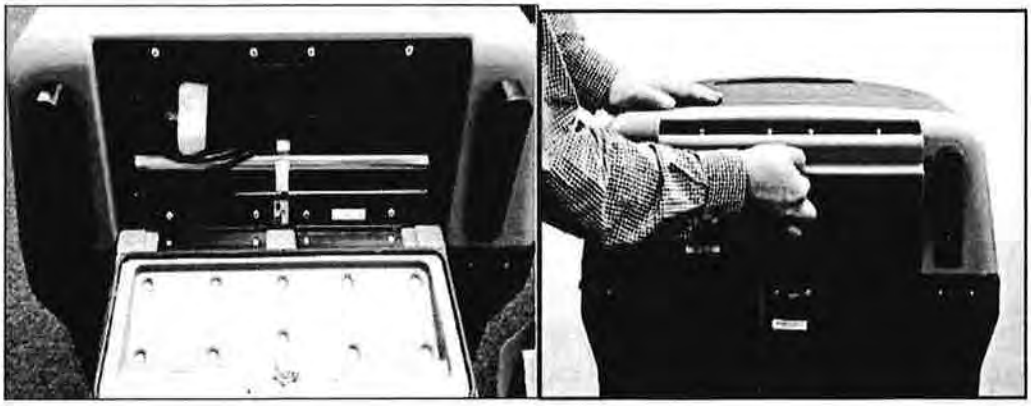
Rear

26. Extend the roller handle and lift the handle to shift the weight of the Ballot Transfer Bin to the rear wheels. **The Ballot Transfer Bin will remain sealed and will be transported to the local board of elections office by closing judges (or chief judges if closing judges are not assigned).**

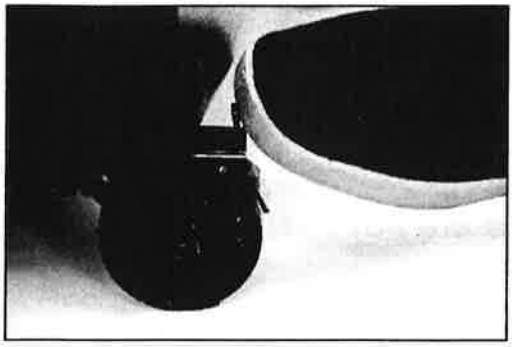


Packing the Scanning Unit

1. Pack the power cord with the grey surge suppressor into the back compartment of the Scanning Unit. Close and lock the back compartment door.



2. Release the parking brakes by tapping vertical metal tabs forward with toe. **Caution: The metal tabs are sharp.**



3. Two election judges roll the Scanning Unit to the Transfer Cart to be loaded for return to the local board of elections.

Packing Other Supplies

Closing Judges (or Chief Judges if closing judges are not assigned) will return a Memory stick (in locked red bank bag), Ballot Transfer Bin(s) with voted ballots, Completed Forms Envelope (containing all completed forms), Orange Provisional Ballot Bag, EPollbooks and VAC Envelope with Voter Authority Cards (bundled in groups of 25).

You will also need to return the second memory stick (from the back compartment of the Scanning Unit) in the locked Clear Bank Bag with your technician.

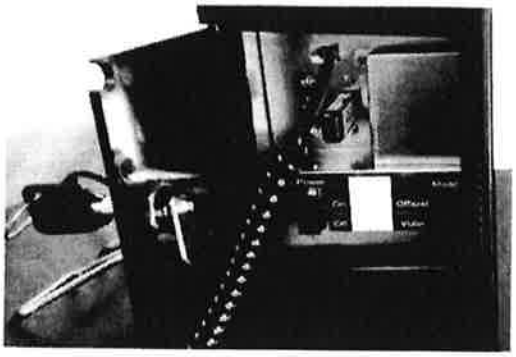
18. Return the carrying case to the Transfer Cart. Return the key and *Ballot Marking Device Integrity Report* to a chief judge.

Closing the Ballot Marking Device

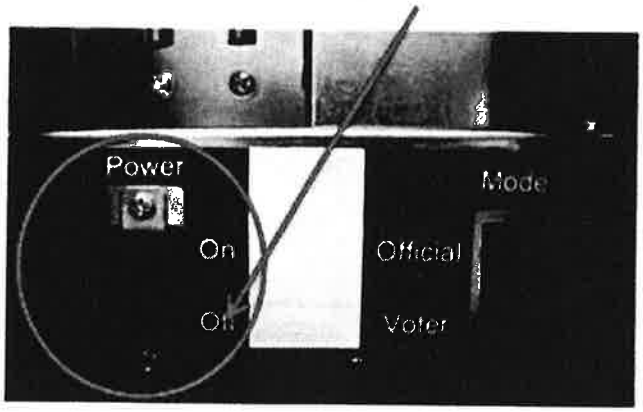
1. Remove the privacy screen.

2. Record the side compartment tamper tape number in column D of the closing section of the *Ballot Marking Device Integrity Report.*

3. Remove the tamper tape from the side compartment. Use the round BMD key to unlock and open the side compartment door.

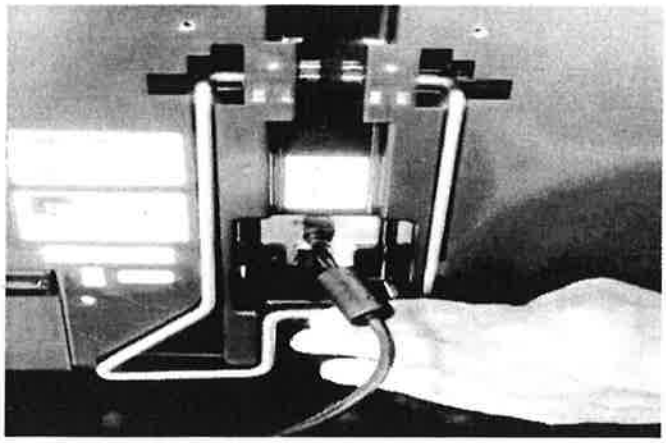


4. Flip the **"Power"** switch to the **"Off"** position.

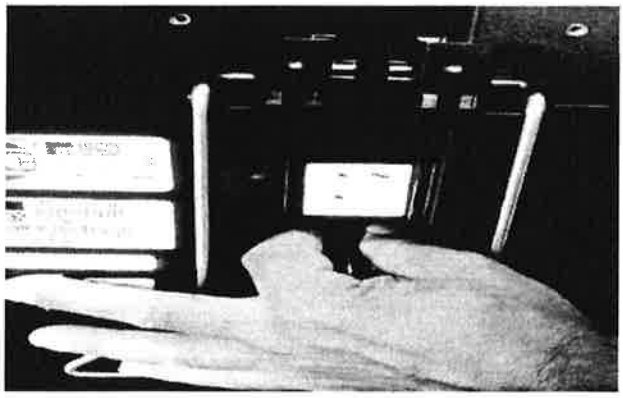


5. Close and lock the side compartment. Apply new tamper tape and record the number in column E of the *Ballot Marking Device Integrity Report.*

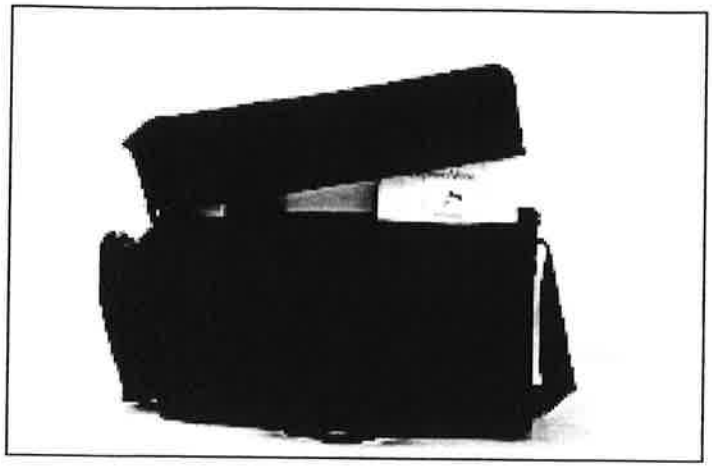
6. Close the stand on the back of the BMD. It will snap into place.



7. Remove the power cord from the back of the BMD by sliding the sheath on the plug back while gently pulling the plug out.



8. Pack up the BMD. Place the keypad, and headphones back into the carrying case. Return the power cord to the carrying case side pocket.



9. Return the BMD to the Transfer Cart. Sign and return the *Ballot Marking Device Integrity Report* to a chief judge.

EXHIBIT E

Wait times, arrival to Check-in at e-Pollbook

NOVemBeR 6, 2012 PResi DeNtia L GeNeRaL eLeCti ON

Prince George's County, mD Precinct 17-01 mt. Rainier elementary school

Chief judges were instructed to report wait times longer than 90 minutes to the county board of elections. No directions were provided for how to assess wait times other than informal estimates. We decided to gather the data in a more precise way.

DATA COLLECTION METHOD

Arriving voters were periodically handed slips of paper with their arrival time written on it and instructed to give it to the election judge at check-in. Check-in judges wrote the current time on the paper and gave it to chief judges. After check-in they usually had to wait an additional 10 to 20 minutes for a DRE to become available but we did not fornally gather that data.

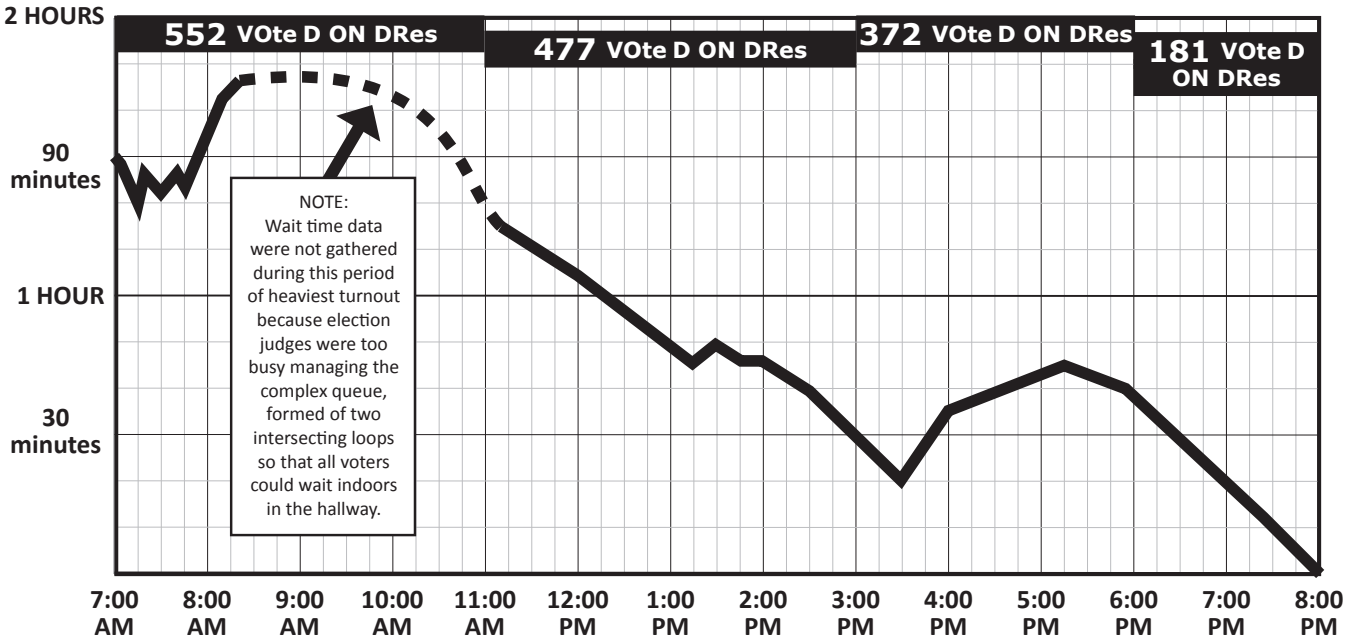
TURNOUT

51% of voters registered in this precinct (1582 of 3112) voted on DREs on election day.

BALLOT LENGTH

The ballot contained 21 contests, including 7 state ballot questions and 7 county ballot questions.

EQUIPMENT

Thirteen DREs were deployed in this precinct. One had to be removed from use at approximately 2:45pm because of calibration problems with the touchscreen.

Arrival Time	Check-in Time	Wait time (mins)
7:00 AM	8:30 AM	90
7:05 AM	8:34 AM	89
7:15 AM	8:35 AM	80
7:20 AM	8:45 AM	85
7:25 AM	8:46 AM	81
7:40 AM	9:05 AM	85
7:45 AM	9:07 AM	82
8:11 AM	9:52 AM	101
8:20 AM	10:05 AM	105
11:10 AM	12:25 PM	75
12:00 PM	1:05 PM	65
1:15 PM	2:00 PM	45
1:30 PM	2:20 PM	50
1:45 PM	2:30 PM	45
2:00 PM	2:45 PM	45
2:30 PM	3:10 PM	40
3:00 PM	3:30 PM	30
3:30 PM	3:50 PM	20
4:00 PM	4:35 PM	35
5:17 PM	6:02 PM	45
5:55 PM	6:35 PM	40
7:23 PM	7:35 PM	12