VOTING SYSTEM SECURITY RECOMMENDATIONS FOR HOUSE ELECTIONS STUDY COMMITTEE

Prepared by VoterGA – November 24, 2025 - FINAL

Table of Conclusions

I. BACKGROUND

The House Blue Ribbon Study Committee on Election Procedures was established by Speaker Jon Burns at the end of the 2025 legislative session. The committee's objective is to study and evaluate Georgia's current laws, policies and procedures for administering Georgia elections. The committee was also tasked to analyze the statewide and local elected officials and boards that oversee the administration of our elections.

The committee members are:

- Rep. Tim Fleming - Chairman
- Rep. Victor Anderson - Vice Chairman
- Rep. Martin Momtahan
- Rep. Trey Kelley
- Rep. Rob Leverett
- Speaker Pro Tempore Jan Jones
- Rep. Saira Draper

The committee held 6 meetings around the state from July 15 to October 16 of 2025. At each meeting, members heard from speakers on a variety of important election topics and we are grateful that we were invited to speak on current and future electronic voting security. We commend all of the members for listening intently and asking thoughtful questions. It must be noted however, that our followers expressed serious concerns about how Rep. Draper used much of her time to conduct partisan personal attacks on SEB Vice Chair, Dr. Jan Johnston, SEB member Janelle King, expert witness Mark Davis, Chief Executive Officer and Certified Public Accountant Erik Christensen, and expert witness Garland Favorito, author of this study.

This study was prepared to provide the committee with an historical perspective on voting system security issues, current vulnerabilities and vote counting failures. Once armed with a historical perspective and full knowledge of current system issues, the committee will then be equipped to distinguish between real and fake solutions needed to enhance Georgia election code.

The study relies heavily on court documents and rulings, expert witness testimony, forensic analyses and state commissioned studies. It strives to avoid academic theories, non-professional opinions and certainly, artificial intelligence. The original study released on November 7, 2025 has been enhanced with additional solutions and proposed legislative changes as well as additional federal compliance considerations in this final version.

Elections in its simplest form must accurately authenticate ballots, voters and counts. While the Georgia General Assembly has made landmark strides in achieving these goals with over two dozen legislative enhancements in the last five years there is still more work to be done. Georgia must end secretly counted elections using secret proprietary software with secretly preserved ballots cast by voter data outsourced to a secret third party location.

II. HISTORICALLY RELEVANT ELECTION SECURITY ISSUES

1. 2000–2002, GEORGIA IMPLEMENTS A PAPERLESS VOTING SYSTEM

a) In 2000, 82% of Georgia voted on verifiable ballots

At the turn of this century, approximately 82% of Georgians cast ballots on verifiable optical scan or punch card systems while roughly 17% cast their ballots on unverifiable lever machines. In January of 2001, after intense media hype over the 2000 Florida presidential election recount, former Secretary of State (SOS), Cathy Cox, produced a report entitled *"The 2000 Election: A Wake-Up Call for Change and Reform".*

In February 2001, Sen. Jack Hill introduced SB213, in pertinent part *"…to authorize the Secretary of State to conduct a pilot project to test electronic recording voting systems during the 2001 municipal elections…"* and *"…to create the Twenty-first Century Voting Commission…".* On March 21, 2001, the General Assembly passed SB213 as amended by the House. The bill was signed by the governor as Act166 of the Georgia Legislature on April 18, 2001 and it included the provision that: *"Such voting systems shall be required to have an independent audit trail for each vote cast."*

b) In 2001, a voting system evaluation was conducted of mostly paperless voting systems

In June 2001, the 21st Century Voting Commission authorized seven Direct Recording Electronic (DRE) voting system vendors to participate in a pilot and the SOS Office entered into contracts with the six certified vendors to provide equipment and support for the pilot projects. The vendors were Diversified Dynamics, Election Systems & Software, Global Election Systems (GES), Hart InterCivic, Shoup Voting Solutions, and Unilect. GES was purchased by Diebold in 2002. The evaluation was led by Kennesaw State University Professor Britain Williams.

In December 2001, the 21st Century Voting Commission issued a report that documented pilot project experiences and made recommendations for the future. One recommendation was that such machines *"have an independent paper ballot audit trail for each vote cast".* Two vendors, Avante and TruVote, offered technology that would likely meet the recommendation of the commission and the legal requirement of Georgia Act 166 but neither were seriously evaluated. In January 2002, the Georgia Technology Authority issued a Request for Proposal (RFP) that was drafted by the SOS office. Secretary Cox's Request for Proposal did not contain the 21st Century Voting Commission recommendation or the legal requirement for an independent audit trail of each vote cast.

c) DRE issues raised for verifiability, auditability, recount capability and transparency

On February 6, 2002, Mr. Favorito, the author of this study, wrote to then Assistant SOS Michael Barnes to inform him that the Request for Proposal for a new DRE system had no requirement for voter verifiability of their ballot. He explained that such a requirement is *"mandatory to protect Constitutional rights of voters as well as to preserve open, honest and free elections"*. He explained five ways how *"electronic voting machines can easily be programmed to distort voting results and still go undetected in pre-election tests or certifications"*. He also explained the lack of an audit trail in most of the proposed systems and advocated for unique ballot identifiers for each ballot.

Many others raised issues about the paperless voting systems being evaluated as well. Fulton County Elections Director Cynthia Welch, wrote to Secretary Cox to explain that a paperless system could not recount an election properly.

d) In 2002, a paperless DRE system was purchased and implemented in 6 months

In February of 2002, Sen. Jack Hill introduced SB414 in pertinent part *"…to provide that the state shall provide a uniform system of direct recording electronic voting equipment for use by counties in the state by 2004…".* The General Assembly passed SB414 as amended by the House on April 12, 2002 and it was signed into law as Act 769 by the governor on May 9, 2002, **without the original SB213 requirement for an independent audit trail of each vote cast.**

On January 23, 2002, Diebold announced that it had completed an acquisition of Global Election Systems. On May 3, 2002, former SOS, Cathy Cox and former Georgia Technology Authority Director, Larry Singer, entered into a $54 million contract with Diebold to purchase electronic voting equipment that did not meet the provision of Act 166 stating*: "Such voting systems shall be required to have an independent audit trail for each vote cast."* Diebold was represented by lobbyist Lewis Massey who served as the former SOS when Cathy Cox served as his assistant during that time. Massey, a Democrat, later joined with Bruce Bowers, son of former Republican Attorney General (AG) Michael Bowers to form a lobbying partnership entitled Massey Bowers LLC which was then able to lobby effectively on both sides of the political spectrum as the SOS office changed hands in 2006.

On May 9, 2002, Governor Barnes signed SB414 into law as Act 769 of the Georgia Legislature. An additional $4 million above the initial purchase was appropriated for electronic voter education and distributed to civic groups such as League of Women Voters and Common Cause of Georgia. **The entirely new technology was implemented in less than six months**. In November 2002, Georgia became the only state in the U.S. to conduct statewide elections on electronic voting machines. The paperless system contained no physical ballot despite the Constitutional requirement that: *"Elections by the people shall be by secret ballot and shall be conducted in accordance with procedures provided by law."* [Art. II, Sec 1, Para. 1]

e) The paperless DRE system transformed Georgia from 82% voter verifiability to 0%

Installation of the paperless voting system eliminated in-person physical ballots from Georgia elections and removed transparency from Georgia's in-person electoral process. Without ballots there is no transparency. Voters cannot verify selections, election officials cannot audit results and candidates cannot request a legitimate recount because the system can only reprint previous unverifiable results. **Installation of the paperless DRE transformed Georgia from 82% in-person verifiability to 0%, effectively disenfranchising all Georgia voters who vote in person.**

f) The 2002 election had stunning upsets in the Senate and Gubernatorial races

The 2002 election saw stunning upsets in the Senate and Gubernatorial races. Republicans Sonny Perdue, who defeated incumbent Roy Barnes for Governor, and Saxby Chambliss, who defeated SOS Max Cleland, trailed significantly in Election Day polls. Nearly all other down ballot races went to Democrats. Sean Hannity referred to it on a Fox News program as the *"Earthquake in Georgia".*

g) VoterGA depositions found system was patched and not recertified as required by law

In July of 2006, VoterGA was formed and a group of its Plaintiffs filed suit. The amended complaint contained **13 separate counts,** each challenging the legality or constitutionality of the electronic voting equipment installed in Georgia during 2002. **A sworn deposition taken from Professor Williams revealed that the President of the voting system vendor had personally installed a software patch on Fulton and DeKalb County voting equipment and that patch was not recertified as required by law.**

h) Georgia Supreme Court upholds paperless voting despite Constitutional ballot requirement

On September 8, 2008, Fulton Superior Court Judge Michael Johnson held a hearing on summary judgment motions and dismissed the Plaintiffs' case even though facts of the case in dispute should have mandated a trial. Judge Johnson promised a written ruling within five days but that ruling was not produced for months and only then after a state legislator called his office to request it. Once Plaintiffs reviewed Judge Johnson's ruling they found what they believed to be 17 conclusions that had no basis in the facts or evidence of the case. On or about March 30, 2009, the Plaintiffs filed a notice of appeal directly to the Georgia Supreme Court. The grounds for the appeal were that:

- The court misapplied key case law that establishes voting as a fundamental right protected by both U.S. and Georgia Constitutions.
- The court denied the Plaintiffs' right to a trial by making numerous conclusions that conflicted with the evidence in the case.

In October of 2009, the Georgia Supreme Court released a decision denying the Plaintiffs' right to trial even though they disputed 41 assertions made by the Defendants. Legally speaking, the court refused to apply strict scrutiny to fundamental voting rights. It instead applied a minimal standard of scrutiny and ruled that the former SOS had a rational basis for implementing the machines even though she was warned in advance they did not have an independent audit trail of each vote cast as required by law. In regards to the equal protection arguments that Election Day voters are not afforded the same protection as absentee ballot voters, the court ruled that: *"voters must assume the risk of necessarily different procedures"*. The Plaintiffs still contend that procedures between Election Day voting and absentee voting are **unnecessarily** different and **if voters must assume the risk that would automatically be a violation of their equal protection rights.** In essence, the court ruling defied all U.S. Supreme Court case law for ballot counting.

i) U.S. District Court eventually finds DRE system is constitutionally deficient

In October of 2019, a U.S. District Court order found in the *Curling v. Raffensperger* case that the DRE voting system purchased in 2002 was constitutionally deficient and must be replaced. The order in the 2017 case filed by Curling and Coalition for Good Governance Plaintiffs, including VoterGA co-founder Ricardo Davis, confirmed what Mr. Favorito had written to the SOS office prior to the original 2002 purchase.

2. 2007–2008, SEB ELECTION SECURITY INVESTIGATIONS MOVED TO SOS

a) In 2007, HB1112 removed SEB supervisory authority over SOS, politicizing investigations

Prior to 2007, the State Election Board (SEB) had supervisory authority over the SOS office. In 2007, the General Assembly passed HB1112, which was signed into law as Act 706. HB1112 provisions maintained SEB authority over election investigations but removed authority over the SOS office. This allowed SOS Karen Handel to set up an Inspector General's (IG) office under the SOS and wrest control of election investigations from the SEB. The move politicized investigations by allowing the SOS to have sole authority over election investigations rather than a more independent board with members appointed by five different entities. This move proved to jeopardize election security investigations because the SOS has a vested interest in maintaining quiet elections, not necessarily in resolving critical issues when vote count accuracies arise.

b) In 2008, a county certified 947 test votes but SOS blamed a voting system technician

In 2008, the Lowndes County Election Board mistakenly certified 947 test votes in live election results. However, the SOS office prosecuted a voting system technician who was not present for tabulation of the votes nor was in any way responsible for results certification. An Administrative Judge eventually dismissed the charge and the technician filed a counter complaint, but the technician, Laura Gallegos, lost her job, a piece of property and $3500 in attorney fees.

c) In 2008, two race outcomes were reversed after results were manually changed

In 2008, there were major upsets in the Douglas County Sherrif and Commission Chair races by Derrick Broughton and James Quarterman. However, an Election Board member took the results home in a spreadsheet overnight, returned the spreadsheet results the next morning and ordered a voting system technician to enter them into the server. The new results overturned the original results that had Derrick Broughton winning the Sherrif's race and James Quarterman winning the Commission Chair. Instead, the incumbents were left in office and the challengers were left stunned by the reversal. The investigation revealed much of what happened but the IG office never recommended a referral of the board member to the Attorney General's office.

3. 2003–PRESENT, GEORGIA'S SINGLE POINT OF ATTACK VULNERABILITY

a) Georgia is one of only four states vulnerable to a statewide single point of attack

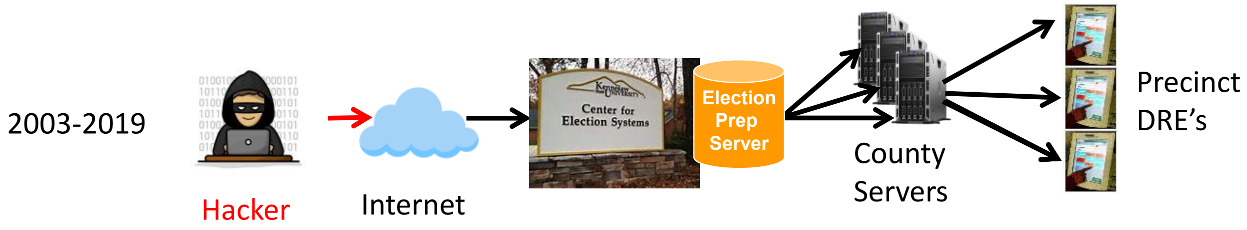
Not long after the 2002 election, a statewide election preparation system was set up at Kennesaw State University (KSU) and managed by the Center for Election Systems (CES), which had a dual reporting responsibility to the SOS office and the KSU Information Technology (IT) division. While advocates of such a centralized statewide system cite advantages in control and uniformity, they fail to consider the significant security risks imposed on the voter. Today, only three other states, South Carolina, Maryland and Louisiana. conduct elections on a statewide voting system, in part, because it exposes the entire election system to a **single point of attack vulnerability.** Dr. Alex Halderman pointed out this vulnerability in January 2024 expert witness testimony during the Curling case.

b) Counties have no means to detect malware received from an exposed state server

A centralized election preparation system leaves the entire statewide voting system vulnerable to a single of attack vector. If the central election preparation server can be compromised, a bad actor can deliver malware in election projects to the counties for every election without detection and distribute that malware to all key county voting system components through the county server. **Counties have no mechanism to detect such malware if received from the SOS election preparation server.**

c) Georgia's election preparation server was installed with a fatal defect impacting all counties

When Georgia's central election preparation server was installed in or about 2003, a Drupal web content system installed on the election preparation server had a defect that exposed the server to easy internet access and allowed anyone technically proficient to take full control of the election preparation server. The defect was so severe it was referred to by IT professionals as "Drupalgeddon", a take-off on the biblical Armageddon. The defect essentially allowed anyone in the world to take over a server running the web content system and control it without detection. Such a defect was present in Georgia's election preparation server for over a decade from the time the web content system was installed at least until 2017



d) In 2016, a security expert notified CES their election prep server was exposed to internet

On August 28, 2016, Logan Lamb, a Bastille cyber security professional, notified CES Executive Director Meryl King that its centralized state election prep server was exposed to internet access to the point where an attacker could gain complete control. Lamb found:

- A current copy of Voter Registration database containing names, addresses and social security numbers for 6.7 million voters;
- Current Elections database(s) that are sent to counties to accumulate election results;
- Windows executables that any recipient can use to create elections databases;
- PDFs of memos containing recent Election Day supervisor passwords;
- Training videos on how to download files, put them on memory cards and insert them into county voting machines.

Lamb determined that the originally installed Drupal Web site Content Management System had security flaws that allow an attacker to have free reign to execute, create, modify and delete any files. It was essentially everything an attacker needs to hack an election without detection or machine access.

An August 2019, U.S. District Court order recognized the significance of this live active election breach: *"Defendants contended that Logan Lamb's ability to access through the KSU CES server multiple gigabytes of voter registration data from CES databases filled with the personal identifying information of millions of*

Georgia voters as well as county and state election staff passwords was not of real significance. The evidence clearly indicates to the contrary."

e) In 2017, the experts noticed the state election preparation system was still exposed

Lamb explained that when he notified Mr. King, King thanked him for the notice, stated he would take care of it and told him to remain quiet about the problem. On March 1, 2017, Mr. Lamb and an associate noticed that the central election preparation server exposure was still not mitigated. This time his associate notified KSU IT and Chief Security Officer (CSO) Bob Gay had IT seize the server, shut it down and turn it over to the FBI for an investigation. KSU issued a March 31 press release stating no illegal activity occurred but no forensic assessment was ever conducted to determine if historical breaches may have compromised past, present or future elections. The CES later discovered they had no backup for the statewide election preparation server that was confiscated by the FBI and KSU had to contact the FBI to retrieve a copy. CES Director Michael Barnes asked Gay to blacklist Lamb & Bastille but later withdrew the request.

f) The election prep server was wiped without a breach analysis when a lawsuit was filed

On April 24, 2017, Gay sent an After-Action Report to King and Barnes that contained notification IT planned to destroy the server data but neither responded. On July 3, 2017, the *Curling v. Kemp*, later retitled *Curling v. Raffensperger,* case was filed largely as a result of the active breach of the central election server. On July 7, all data on the election preparation server was magnetically deleted. On August 8, the case was removed to federal court and on August 9, data on other related CES servers were magnetically deleted. These events are documented in detail in a VoterGA study and the August 2019, U.S. District Court order. [Pg 62-70]

g) SOS Legal Counsel filed a superficial report excusing the server wipe as standard procedure

On October 26, SOS Brian Kemp posted on social media that the server wipes were *"reckless behavior", "inexcusable conduct", "gross incompetence",* and *"undeniable ineptitude"* causing the Attorney General (AG) to cite conflict and resign from defending the Curling case.

Although essentially the legal head of investigations, SOS legal counsel Ryan Germany produced a superficial two-page investigative report on October 30 stating that the server wipe activities were *"standard IT procedures".* **The report ignored SOS investigative standards** because it:

- Failed to identify the complainant for the investigation (likely Sec. Kemp);
- Failed to identify the respondent groups or individuals at KSU who were being investigated as part of the data destruction;
- Failed to identify the elections that were impacted by the data destruction;
- Failed to include the documents he reviewed as exhibits;
- Failed to disclose any KSU individuals who were contacted to investigate the data destruction;
- Initiated no communications with anyone at KSU, CES or IT to investigate the matter during the investigation time period.

The report falsely concluded that: "*"The concern that the data was lost is unfounded"* and " *the narrative asserted in the media that the data was nefariously deleted and is no longer available is completely false and without merit."* **Despite such claims, the server data was never produced for trial.**

h) The U.S. District Court found excuses for the server wipe were *"flatly not credible"*

When a breach or exposure occurs, certain steps must be taken to assess the damage. Tasks that must be performed include activities to:

- Identify the duration of the exposed vulnerability window;
- Determine if an unauthorized breach occurred during vulnerability window by using audit logs;
- Identify the source of the unauthorized breach using IP addresses of the potential attackers;
- Define when the unauthorized breaches may have occurred using log timestamps;
- Assess the impact of any unauthorized breach on the application and its data owners;
- Implement a remediation strategy to compensate for the unauthorized breach.

There is no evidence that any of these standard IT procedures were performed.

In its August 2019 order, the U.S. District Court found: *"the Defendants' contention that the servers were simply "repurposed" and not intentionally destroyed or wiped is flatly not credible".* She added: *"The Defendants have previously minimized, erased, or dodged the issues underlying this case. Thus, the Court has made sure that the past is recounted frankly in this Order, to ensure transparency for the future."* [Pg 152]

i) The SOS directed 2017-2018 security assessments to not include election systems

Under pressure from the most significant exposure in U.S. E-Voting history, the SOS obtained security assessments during 2017 and 2018. Fortalice and its CEO Theresa Payton were retained to conduct the assessments but SOS Chief Technology Officer Merritt Beaver restricted the scope not to include election systems. Assessments were limited to the general SOS external interfaces and did not include election system penetration testing.

The U.S. District court eventually found in its August 2019 order that: "*The core reality is that the State retained neither Ms. Payton nor its other expert, Dr. Michael Shamos, to conduct an actual cybersecurity review and analysis of the GEMS/DRE system and databases or the statewide voter registration system or Elections Division, apart from Fortalice's general risk assessment analysis.*

The Court continued: *"The SOS never asked or contracted with Fortalice to perform a specific cybersecurity evaluation of the security issues facing the SOS elections division and related county election offices, or the security vulnerability and integrity of the GEMS System both within SOS and its county elections counterparts, or the State's voting databases and electronic pollbooks.*

The court further lamented on the absurdity of the contract scope*: "It was outside Fortalice's contract scope to focus on particular Election Division or GEMS data systems or conduct a review of the voter registration system software and operation, or the state election data systems' interface with SOS servers and SOS and County data systems and the cybersecurity and vulnerability issues posed by this interface."*

The court's comments clearly explain the lack of SOS commitment to cybersecurity protection for Georgia voters.

j) The assessment successfully penetrated compromised SOS infrastructure

The U.S. District court again explained in its August 2019 order that: *“The Fortalice/Cloudburst team was able to compromise passwords and escalate its privileges to penetrate the SOS agency data system and access all local work stations and laptops and to establish footholds in a series of internal systems in SOS”.*

The court went on to add: *“Fortalice’s team gained control of domain administrator rights on the Georgia SOS connected network and in turn obtained credentials to identify sensitive data, gained access to network security systems and the system enterprise architecture and system configurations within the SOS.”*
These findings that the SOS infrastructure was compromised were originally withheld from the court and have also been withheld from the General Assembly.

It is still unclear today what vulnerabilities still exist in the SOS office that could affect elections.

k) Only 3 of 22 security risks found by the assessment were addressed a year later

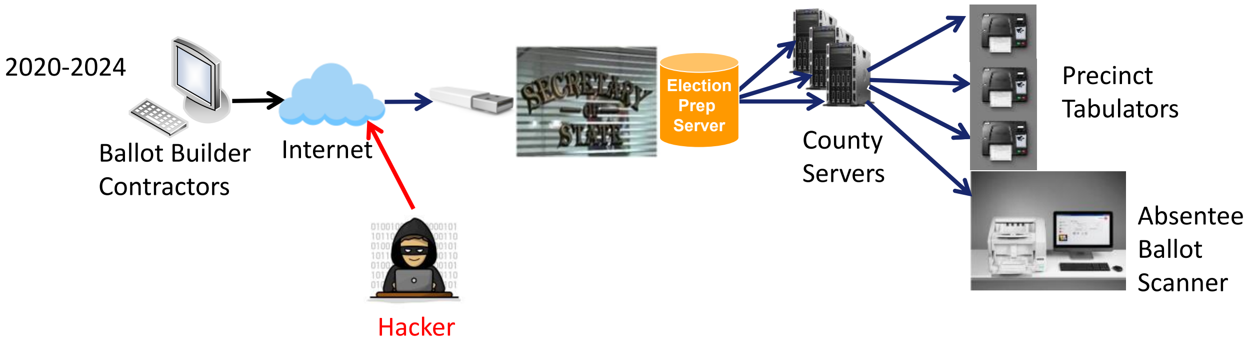
As the court explained: *“The first of the three Fortalice reports dated October 2017 identified 22 cyber security risks to the SOS, with the ten leading ones identified as highest priority for remediation action, including risks associated with password management and security, access control, data security, and network and vulnerability management.”*

A second February 2018 report for the voter registration system found 15 additional serious vulnerabilities. For example, the system used at that time “*does not block connections to the VPN from IP addresses of known threat sources or foreign countries.”.*

The third November 2018 report showed little progress in risk mitigation*. “It found that SOS had fully remediated just three of the 22 deficits identified in October 2017.”* The court added: *“While noting the SOS’s progress, Fortalice made twenty additional cybersecurity recommendations to protect the confidentiality, availability, and integrity of voting and voter data for the citizens of Georgia, fourteen of which were of low to no cost. And it identified the ten top cybersecurity risks from 2017 that carried over through 2018, three of which fell outside the scope of the 2018 assessment requested and were deemed unresolved.* These included insufficient firewall protection, external website vulnerabilities and a lack of controls for identity and access management and voter information privacy. Thus, the cybersecurity risks found in 2017 were never adequately mitigated for the November 2018 General Election.

l) The state election preparation server has always had an internet exposure risk

When the old DRE system was replaced by a BMD system, as explained in the next section, the new single point of attack vulnerability still remained. In addition, the new BMD system continued to have a similar exposure that was identified by Michael Barnes in 2024 sworn testimony. Ballot building contractors transfer ballot definition files through the internet to the SOS office. Mr. Barnes testified that he loads the ballot definitions onto a memory stick which he then inserts into the election preparation server to upload the new ballot definitions.



4. 2018-2019, GEORGIA PURCHASES A NEW UNVERIFIABLE VOTING SYSTEM

a) In 2018, the Lt. Gov. race had the largest unexplained undervote in electronic voting history

The 2018 General Election for Lieutenant Governor produced the largest still unexplained undervote in electronic voting system history. Sara Riggs Amico, the Democrat candidate for the office received far less votes than other down ballot candidate Democrats for no obvious reason during her race with Geoff Duncan. An analysis of the race indicates that the DRE touchscreen voting system sporadically non-displayed the race in heavy Democrat or minority dominated precincts. A VoterGA study entitled, "*Unresolved Security Risks of Ballot Marking Devices*", documents the unexplained anomalies in this race as well as the inherent risks associated with Ballot Marking Device (BMD) systems. Georgia had no audit provision at the time and there is no way to audit what a touchscreen showed to the voter.

b) In 2018, the SAFE Commission was established to select a new voting system

In April of 2018, Governor Brian Kemp established the Secure Accurate Fair Election Commission (SAFE) to select a new voting system. The SAFE Commission consisted of a variety of appointees and it held a series of meetings throughout the state. The Commission received expert opinions and a National Academies of the Sciences report advocating the use of hand marked paper ballots. VoterGA presented recommendations to the SAFE Commission in December, 2018 and produced a January 17, 2019 report of those recommendations.

c) The Commission recommended BMDs despite objections from their technical expert

In January of 2019, the SAFE Commission made recommendations to the legislature including the recommended use of BMDs. That recommendation was controversial in particular because the cyber security expert appointed to the commission, Wenke Lee, vehemently objected to it. Dr. Phillip Stark, the inventor of Risk Limiting Audits, had written to election officials that RLAs, and audits in general, cannot be effective on BMD systems because there is no original source of voter intent among other reasons.

d) HB316 passed and mandated use of BMDs statewide without initial or ongoing fiscal notes

In March of 2019, the General Assembly passed HB316 which mandated statewide BMDs. The $150 million estimated expenditure was signed into law **without the required fiscal note** for initial expenditures of $5 million or more. The $10 million per year unfunded mandate on the counties for maintenance, testing, licensing and logistics was also approved **without the required fiscal note** for ongoing expenditures of

$100,000 or more. The decision to ignore fiscal notes was made by the presiding officer of the Senate, Geoff Duncan, who was declared the winner of the highly controversial 2018 Lieutenant Governor's race previously mentioned.

e) In June 2019, the Dominion Democracy Suite 5.5 system was purchased for $107 million

In June of 2019, Secretary of State Brad Rafensperger, who had won election in 2018, and Gabriel Sterling, who he had hired as a deputy at that time, signed a contract to purchase the Dominion Democracy Suite 5.5 -A (GA) system even though that system had been rejected by Texas for security reasons. The contract required use of unverifiable bar-coded vote tabulation where votes are embedded in a proprietary Quick Response (QR) code that cannot be read by a voter even with a QR code reader. The SOS was warned personally by this author not to purchase an unverifiable QR coded vote tabulation system in 2018 prior to him becoming SOS.

f) The Dominion contract was issued with a 20-year bond for a system with a 10-year shelf life

The Dominion system was purchased with a 20-year bond included in the annual budget. However, the system has only a 10-year expected shelf life meaning that **Georgia taxpayers will still be paying for the system 10 years after its useful life expires.**

g) In October 2020, a U.S. District Court found the BMD system violated two Georgia statutes

In September 2020, Colorado announced that it would replace its QR coded vote tabulation that Georgia was just about to implement. in October 2020, a U.S. District Court found in the *Curling v. Raffensperger* case that the system violated two Georgia statutes for voter verifiability. Georgia's voting system must:

- *"…print an elector verifiable paper ballot"* - O.C.G.A. § 21-2-2(7.1);
- *"…produce paper ballots which are marked with the elector's choices in a format readable by the elector"* - O.C.G.A. § 21-2-300(a)(2)

The court found in its order that:

- *"Plaintiffs and other voters who wish to vote in-person are required to vote on a system that does none of those things."* [Pg 82-83]

However, no relief was granted in the matter and **the November 2020 election was conducted on a voting system that the U.S. District Court found was not in compliance with Georgia laws.**

5. THE 2020 ELECTION

h) Millions of dollars in private funds influenced the 2020 election and jeopardized its security

During 2020, the Mark Zuckerberg funded Center for Technology and Civic Life (CTCL) provided $45 million in politically partisan funds to Georgia counties. Mr. Zuckerberg spent over $330 million to establish CTCL, which employed as its policy director, David Plouffe, a former Obama campaign manager who wrote the book entitled: *"A Citizen's Guide to Beating Donald Trump".*

The "Zuckerbucks" were spent mostly on partisan get out the vote efforts, installation of unsecure drop boxes that allowed dubious ballots to be injected into the election and technical resources used to gain control of electronic voting equipment in some counties like Fulton. These objectives are shown in the standard CTCL contract terms. True the Vote GEO trafficking evidence and county surveillance videos show potential ballot trafficking operators injecting ballots through drop boxes often multiple times in the middle of the night.

A capital research report summarizes the political bias in the allocation of $45 million given to Georgia counties in finding that over 94% of the money went to counties won by Joe Biden, including all of the 10 largest county grants. The study suggest that this funding may have resulted in a 200,000 net increase in voter turnout.

Fulton County utilized the CTCL funded Elections Group to provide technical assistance that produced the still dubious 2020 General Election results. A December 3, 2020 Email from Fulton Co. Elections Director Richard Barron to Ryan Macias of the Elections Group contained a Batches Loaded Report XML that Fulton had difficulty reconciling. The Email indicates that the Elections Group was involved in producing final certified Fulton County election results that are still in question today.

i) The 2020 Georgia General Election was the most controversial since 2002

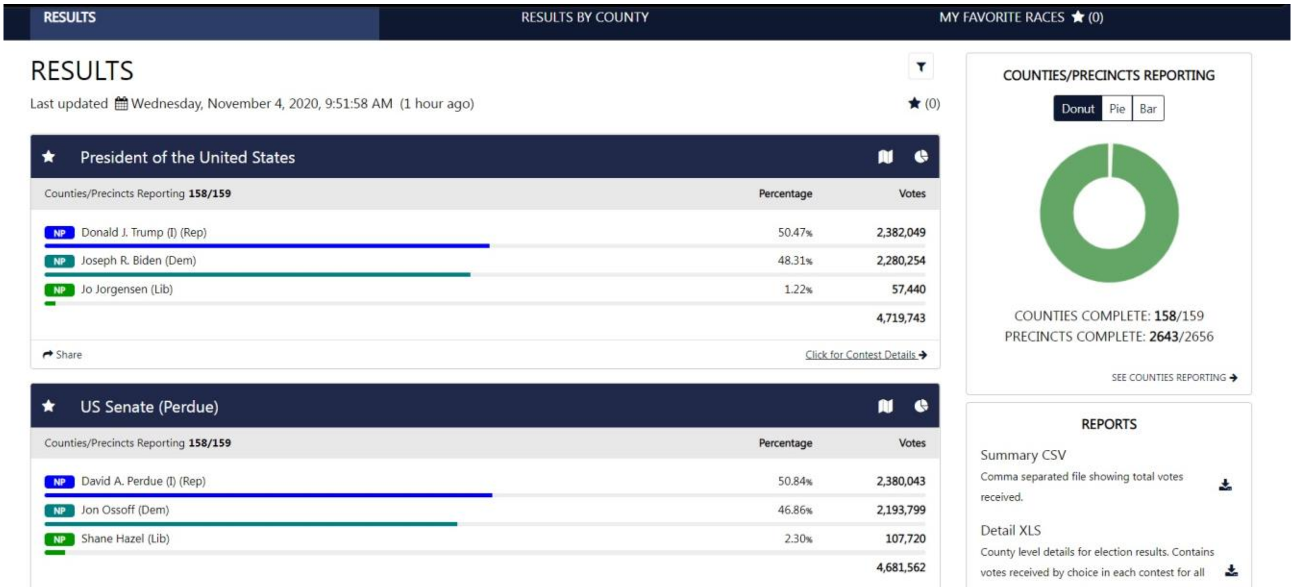
On November 3, 2020, Georgia conducted its most controversial election since 2002. The election had over 30% mail-in ballots and several serious vote counting failures described later in this study. The two statewide federal elections were particularly close. Vice President Joe Biden was declared the winner over President Donald Trump by 11,779 votes. Senator David Perdue was thrown into a runoff with challenger Jon Ossoff by just over 26,000 votes according to the certified recount results.

j) The SOS confirmed to NBC 4.7 million total ballots were cast and Trump would win

On the morning after the 2020 General Election at about the 8 a.m. hour, Secretary Raffensperger was interviewed on the NBC today show. When asked about the status of the election results, he replied: *"We don't guess", "4.7 million voters voted",* there are *"about 2% left"* to count, counties will *"get that done today",* and it *"won't change any of the outcomes" "…even if one of the candidates got 100% of the votes it wouldn't be enough".* At that time with 98% of the votes counted and only about 94,000 votes left to count, the NBC graphic showed President Trump with a 103,705-vote lead over then Vice President Joe Biden.

k) SOS results with 99 1/2 % reporting show Trump and Perdue with insurmountable leads

Just before 10 a.m., and about two hours after the interview, the Clarity Elections results publishing system used by the SOS, confirmed his statements. By then, all of the 159 counties except Fulton had reported and only 13 precincts were left to count in Fulton. With only about 10,000 votes left to count and 99 1/2% of Georgia reporting, the results publishing system showed President Trump with an insurmountable 101,795 vote lead and Senator David Perdue with an insurmountable 78,523 vote margin over the runoff threshold.



RESULTS

Last updated Wednesday, November 4, 2020, 9:51:58 AM (1 hour ago)

★ (0)

President of the United States

Counties/Precincts Reporting **158/159**	Percentage	Votes
NP Donald J. Trump (I) (Rep)	50.47%	2,382,049
NP Joseph R. Biden (Dem)	48.31%	2,280,254
NP Jo Jorgensen (Lib)	1.22%	57,440
		4,719,743

Share

Click for Contest Details

US Senate (Perdue)

Counties/Precincts Reporting **158/159**	Percentage	Votes
NP David A. Perdue (I) (Rep)	50.84%	2,380,043
NP Jon Ossoff (Dem)	46.86%	2,193,799
NP Shane Hazel (Lib)	2.30%	107,720
		4,681,562

COUNTIES/PRECINCTS REPORTING

COUNTIES COMPLETE: **158**/159
PRECINCTS COMPLETE: **2643**/2656

SEE COUNTIES REPORTING

REPORTS

Summary CSV
Comma separated file showing total votes received.

Detail XLS
County level details for election results. Contains votes received by choice in each contest for all

l) A month later, 5 million ballots were certified overturning Senate and Presidential results

On December 4, 2020, the SOS certified 4.998 million Presidential and Senate votes on over 5 million ballots cast. The additional 200,000+ ballots accepted and counted after Election Day overturned the election results of the Senate and Presidential races as posted on the day after the election. **The SOS has still offered no public explanation as to where these 200,000+ phantom ballots came from.**

6. AUDIT AND SURVEY DISCREPANCIES

a) On Nov. 11 the SOS ordered a full hand count of the Presidential race to meet state law

At the time of the 2020 election, Georgia law required only one race to be audited every two years and that race could be selected by the SOS, not randomly. On November 11, 2020, Secretary Raffensperger ordered a full hand count of the 2020 Presidential election. That was an excellent choice because of the closeness of the race and the high-profile nature of the race. It was also important to use a full hand count of the ballots in lieu of Georgia's normal Risk Limiting Audit technique because the closeness of the race would have required a very high number of ballots to be audited and randomly selecting those ballots would consume far more time than simply counting the race.

b) On Nov. 14, the audit was conducted with a broken chain of custody that invalidated it

As a statewide audit monitor coordinator, the author can confirm that the 2020 hand count audit was riddled with simple and complex problems that invalidate it based on generally accepted auditing practices. For example, some counties such as Fulton County, placed members of the same political party on two-person teams to count the votes and produce tally sheets of the counts rather than separating political party members into different teams. That approach facilitated collusion rather than preventing it.

In many major counties, tally sheet data entry points were unmonitored, allowing data entry personnel to enter any totals for the races they wanted without detection regardless of what counts were on the tally sheets. Fulton County had only a single person uploading all counts from the auditors' tally sheets into the SOS ARLO system and that person could enter whatever counts he chose without detection. When I approached the Fulton County Elections Director about monitoring the upload point, he told me that they were not allowing that. Such a position conflicts with Georgia election transparency law. O.C.G.A § 21-2-406.

But most importantly, when counties entered tally sheet results into the SOS ARLO system, the counties were left with no electronic record of their own audit. This allowed the SOS office to report any totals they wanted to make audit results match original results without detection if they chose to do so. **Such a process has a clear broken chain of custody in the middle of the audit that invalidates the entire audit in every county by any generally accepted audit practice.**

c) Senior poll managers and audit monitors found counterfeit Fulton ballots during the audit

This author was present on November 14, 2020, when four senior poll managers and two audit monitors discovered counterfeit absentee ballots during the Fulton County audit process and were told by Fulton election officials to keep counting those ballots anyway. These counterfeit mail-in ballots were not folded from being mailed, not written with a writing instrument, not on standard ballot stock and marked identically on all races for dozens of ballots in a row. All six signed sworn affidavits the next night after the hand count finished.

The SOS attempted to privately claim that these ballots may have been emergency ballots or ballots duplicated because they are damages or are Uniformed Overseas Citizens Absentee Voting Act (UOCAVA) ballots. However, voters in only one Sandy Springs precinct, not related to the counterfeit ballots found, cast a few emergency ballots. Furthermore, this author was present for ballot duplication and can confirm that any ballot duplication was done using BMDs which produce a completely different in-person selection summary from an absentee ballot style. Thus, there is still no explanation for the counterfeit ballots.

d) On Nov. 20, the SOS certified the original results claiming that the audit confirmed them

The Georgia SOS engaged the Carter Center to monitor the 2020 hand count audit in several key counties. Amazingly, the Carter Center found none of the problems described in this section. The Carter Center audit observations falsely concluded on behalf of the SOS: *"This report finds that the RLA confirmed the original results of the presidential election in Georgia."* On November 20, the Georgia SOS certified the original election results, claiming that the audit confirmed them. It is inconceivable that the Carter Center could have been inept enough to have missed such critical, devastating audit problems.

e) On Dec. 10, a Senate Committee confirmed the results should have never been certified

Throughout December 2020, the House Government Affairs Committee and the Senate Judiciary Subcommittee on Elections conducted hearings on the 2020 General Election. Many witnesses testified to both committees. On Dec. 10, 2020, the Senate Judiciary Sub Committee on Elections produced a report concluding from testimony that: *"The election was so riddled with fraud, errors and irregularities it should have never been certified."*

f) Gov. Kemp's 36-point study found Fulton Co. audit results did not confirm original results

On November 18, 2021, Governor Brian Kemp sent a letter to the SEB requesting them to investigate the 2020 Fulton County audit. His letter and supporting study is based on discrepancies provided to him by a citizen, Joe Rossi, who concluded that there were 6,659 ballots added to the Fulton 2020 hand count audit to make the audit results match the original results. Gov. Kemp's letter referred to the SOS audit data as "sloppy" and "inconsistent". Gov. Kemp attached for the SEB his 36-point study of inconsistencies in the audit data which illustrate how the audit could not have possibly confirmed the original election results.

g) Gov. Kemp's study was based on VoterGA research that uncovered massive audit problems

The discrepancies in Gov. Kemp's study were based on VoterGA research released on July 13, 2021. That research was conducted by a team of volunteers led by David Cross. It found massive discrepancies in the Fulton audit including:

- An analysis of Fulton's 2020 ballot images found that 60% of the tally sheets had incorrect totals that did not accurately represent the actual counts which should have been produced from the ballot images;
- An analysis of the audit report detailed double reported votes on over 4,000 ballots;
- An analysis of the tally sheets found seven falsified tally sheets were created containing a total of 800 votes for Joe Biden and none for Donald Trump and Libertarian l candidate Jo Jorgenson even though the ballot images show a more normal distribution of results between the candidates;
- Analysis of the ballot images further found hundreds of double scanned and double counted ballots were included in the hand count audit. This number of double scanned double counted ballots was later determined to be roughly 3,950 as explained in expert testimony by 30-year image analyst Phillip Davis at the July 7, 2024 SEB meeting.

h) A VoterGA study found Fulton ballot images were electronically altered prior to certification

On March 7, 2022, VoterGA release another study of the meta data for the 2020 absentee ballot images produced by Fulton County in discovery. It showed that 17,724 certified Presidential votes had no source ballot images. It also showed that all 374,128 original in-person ballot images were missing. Another 132,784 absentee images had no corresponding SHA authentication files and could not be authenticated. The meta data shows that 104,994 images had impossible duplicate time stamps. In all there were 15 different points that conclusively prove the certified published election results cannot be trusted.

i) A SEB investigation found certified Fulton Co. votes for up to 58,924 unsourced ballots

In 2022, one of several complaints against Fulton County's handling of the 2020 election, SEB2023-025, was filed with the SEB by Joe Rossi and Kevin Moncla. This case was supposedly investigated for years and eventually presented to the SEB in its May 2024 meeting. Instead of the normal lead investigator presentation, the case was presented to the SEB primarily by SOS legal counsel Charlene McGowan who told the SEB there was no evidence of violations. Unconvinced, the SEB heard in its July 9, 2024 meeting from three expert witnesses selected by the complainants in the case despite multiple efforts by Chairman Fervier to block their testimony. The experts corroborated the bulk of allegations made in the complaint:

- 17,852 ballots with cast vote records had no ballot images which are required for vote tabulation;
- 20,713 ballots with certified votes have no source tabulator needed to originate them;
- 3,125 double-scanned and double counted ballots;
- 17,234 unsourced ballots were batch uploaded and backfilled into election results by the Center for Technology and Civic Life (CTCL) funded Elections Group to reconcile inexplicable errors.

This author has been at each SEB meeting over the last few years in an attempt to help have this case investigated properly but instead, witnessed how Chairman Fervier has intentionally tried to sabotage investigative efforts of the majority of board members. Just a few examples include:

- Changing the schedule of the May 7, 2024 case presentation to ensure that member Rick Jeffares would not be present to second Dr. Johnston's motion to refer SEB2023-025 to the AG;
- Calling for an inappropriate Executive Session in the July 9, 2024 meeting in an attempt to prevent expert witness testimony on behalf of SEB2023-025 complainants;
- Failing to close the July 10, 2024 meeting properly which would have expunged the expert witness testimony from the record had the board members not called another meeting to properly close it.
- Falsely claiming in the July 9, 2024 meeting and other meetings that the SEB had closed the case during its May 7 meeting and could not reopen it;
- Falsely claiming in the July 9, 2024 meeting and other meetings that the SEB had already adjudicated the case during the May 7 meeting even though the SEB is solely an investigative body that has never had adjudicating authority since its creation in 1964;

The chairman's failure to close the July 10, 2024 meeting properly led to a lawsuit against the SEB when they had to hold a July 12 meeting to properly close it and the chairman failed to ensure the notice was posted. The chairman also failed to oversee timely ORR processing resulting in a lawsuit against the SEB and Dr. Johnston who was not even the recipient of the original ORRs.

SEB2023-025 is the most important case the SEB has considered since its inception. It contains more serious and far-reaching potential violations than all other SEB cases. The SEB2023-025 examples cited are just a few of the repeated attempts the chairman has made to undermine the will of the SEB majority. Although the committee has vocalized that the SEB has problems, it needs to understand the source of those problems since it has authority to appoint a new SEB chair when the session reconvenes.

j) Fulton County did not perform legally required envelope signature matching in 2020

Georgia experienced a dramatic, inappropriate, statewide reduction in absentee ballot signature rejection rates from 3.47% in 2018 to .34 % in 2020. This was due in part to an agreement the SOS signed with the Georgia Democratic Party. The agreement allowed ballot envelope signatures to be verified against ballot application signatures rather than signatures on file.

Consequently, the SOS decided to conduct an envelope signature match audit. However, he chose to audit envelope signatures for Cobb County rather than Fulton County where many questions immediately swirled around their handling of the 2020 election. The SOS stated: "*We chose to start with Cobb County because it was the only county where the President and his allies had submitted any credible evidence that the signature verification process was not properly done.*" On the contrary, it was Fulton Co. that has two board members who refused to certify the results in large part on the admission by the Elections Director to the board that signature matching was not performed.

Board member Mark Wingate's affidavit and subsequent testimony explain that his refusal to certify was based in large part on the fact that signature matching was not performed. Fulton County later admitted in the Harrison Floyd trial that their BlueCrest signature verification machine was not operating during the 2020 General Election.

Mr. Wingate's testimony is corroborated by Election Assistance Commission (EAC) statistics showing Fulton rejected only 6 of 147,000+ absentee ballots. Had signature mismatch been performed roughly 5,000 ballots would have been rejected as invalid based on normal rejection rates. Since invalid signatures were likely updated into the voter registration file the legislature wisely moved to replace subjective absentee ballot signature matching with more precise Drivers' License ID matching.

k) State Farm Arena video shows double counting and election transparency violations

At the December 3, 2020 Senate Judiciary meeting, the State Farm Arena video of absentee ballot processing was shown to the committee. Although Gabriel Sterling insisted that was *"normal ballot processing"* the video reveals several violations of Georgia law that this author can confirm as a poll monitor at the arena. These potential violations include:

- Unprecedented use of a curved room that obstructs monitor visibility O.C.G.A. § 21-2-406
- Placement of monitors in a corner that obscures visibility of certain activities O.C.G.A. § 21-2-406
- Use of skirted tables that can be used to conceal election material O.C.G.A. § 21-2-406
- Concealing certain boxes of ballots under skirted tables O.C.G.A. § 21-2-406
- Continuing to scan ballots after announcing that scanning will stop O.C.G.A. § 21-2-483(b)
- Duplicate scanning of ballots that were clearly never jammed as claimed O.C.G.A. § § 21-2-374, 21-2-419(c)

As previously explained, Phillip Davis, a 30-year career image analyst, testified and produced a Ballot Integrity Analysis showing that at least 3,950 Fulton Co. 2020 General Election ballots were double scanned and double counted.

l) The SEB found 346 potential Fulton County 2020 General Election process violations

A 2024 SEB investigation of Fulton County includes a chart identifying 346 potential process violations Fulton County committed in the conduct of the 2020 election. These include a variety of missing election documents for tabulation, reconciliation sheets, security seals and much more. Fulton County has been unable or unwilling to produce the required 2020 Election documentation for the SEB.

m) Fulton County has fought for years to conceal the 2020 election ballots from the public

Instead of simply producing the 2020 General Election ballots, addressing the allegations and ending the controversy, Fulton County has fought in court for four years with multiple attempts to conceal the ballots from the public. The ballots are now under subpoena or otherwise requested by two civil suits, at least one criminal suit, the SEB and both the criminal and civil divisions of the Department of Justice (DOJ).

The County has been assisted by the SOS and AG who filed an amicus brief in an attempt to keep the ballots secret. That brief, which contained a significant amount of untruthful information, falsely claimed the court would be committing a felony by allowing the Plaintiffs to visually inspect or receive a copy of the ballots. The false information in the amicus brief was refuted by the Plaintiffs reply brief.

Fulton County and other Superior Court judges have also been blockers. One falsely claimed Plaintiffs don't have standing, another refused to recuse a conflicted judge and several continue to stall the case even after Plaintiffs won a landmark December 20, 2022 Georgia Supreme court decision on standing unanimously without a hearing.

n) Hand counts showed the voting system failed to count 1,642 votes in Gwinnett County

The official 2020 Georgia audit report summary, which was released undated and untitled, shows counting discrepancies in over half of Georgia counties, including significant discrepancies in dozens of counties. For example, the Gwinnett County hand count audit found that the voting system failed to count 1,642 votes. This was further confirmed in sworn testimony during the January 2024 Curling trial.

o) Hand counts showed the voting system flipped 37 votes from Trump to Biden in Ware Co.

The audit report summary showed many different discrepancies such as a 74-vote difference in the Ware County Presidential race. A closer examination of the discrepancy by this author and a county resident from VoterGA revealed that the voting system flipped 37 votes from President Donald Trump to then Vice President Joe Biden. This vote flip is confirmed by the original election results, hand count audit results and confirmation from the Ware Co. elections director that both of those results are correct. When confronted, the SOS admitted that the hand count revealed President Trump was shorted 37 votes, but he never revealed that those 37 votes were originally awarded to Vice President Biden.

p) Counties have no record of a Dec. 2020 PROV&V “audit” the SOS claimed was performed

The SOS claimed that in December, 2020, *“Pro V&V conducted an audit of a random sample of Dominion Voting Systems voting machines throughout the state using forensic techniques, including equipment from Cobb, Douglas, Floyd, Morgan, Paulding, and Spalding Counties.”* First, ProV&V does not conduct audits. They can only perform a health check to make sure the software is still identical to what was originally installed. But more importantly, ORR replies from the counties where the “audit” was allegedly conducted show that ProV&V never visited any of them.

q) An ORR survey found 1.7 million original ballot images destroyed despite retention laws

On March 25, 2021, Gov. Kemp signed Act 9 based on SB202, which, among many other election security measures, made ballot images public record. Shortly thereafter, VoterGA filed Open Records Requests (ORR) to gain access to the ballot images for each county. In November, 2021, VoterGA produced evidence that over 1.7 million original ballot images were missing or destroyed across 70 counties. Federal and State law require all election records to be retained for 22 and 24 months respectively. 52 USC 20701, O.C.G.A. § 21-2-73

r) A VoterGA report found 13 types of outcome determinative fraud, errors or irregularities

A VoterGA report released in May of 2023 ultimately found 13 types of outcome determinative fraud, errors and irregularities throughout Georgia during the 2020 election. In addition to those issues listed previously, this includes missing drop box video surveillance for 181,000+ ballots, invalid chain of custody documents for 107,000+ drop box ballots and 86,860 voters having false registration dates. The voters were shown as voting in the voter history file and had voter registration dates prior to 2016 in the 2020 voter registration file. However, they were not present in the 2016 voter registration file, thus indicating that the votes may not have been cast by legitimate voters.

s) The SOS made up to 42 false statements about the election in a 10-page letter to Congress

On January 6, 2021, Secretary Raffensperger wrote to Georgia Congressional members, Vice President Pence and leaders in the U. S. Senate and House claiming that false allegations about the November 3, 2020 General Election in Georgia were being made by *“the President and his allies”.* The contents of his 10-page letter dramatically contradicted findings by the Georgia General Assembly based on extensive first-hand testimony from three hearings:

- December 3 – Senate Judiciary Sub-Committee
- December 10 – House Government Affair Committee
- December 30 - Senate Judiciary Sub Committee

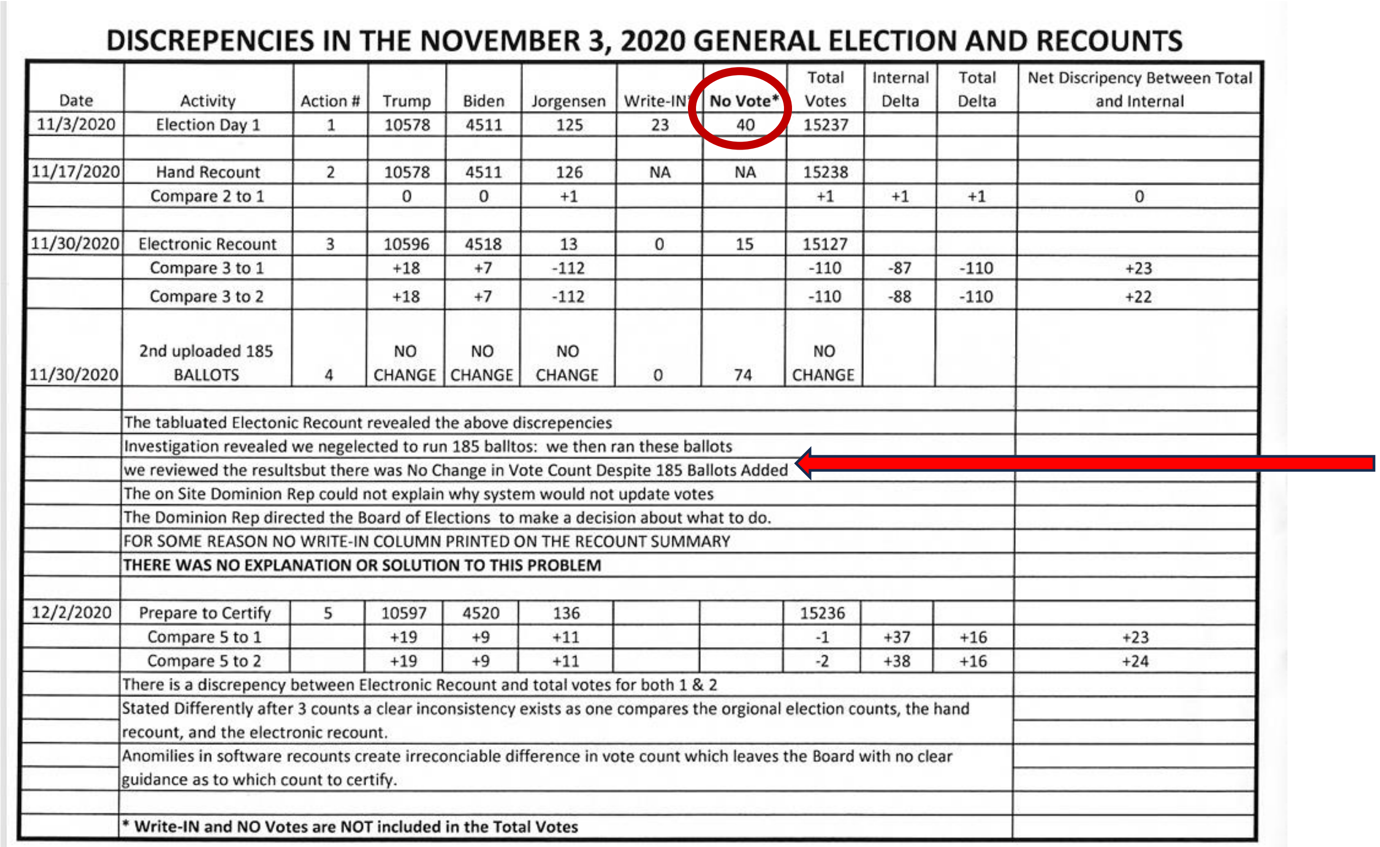
It is now obvious that the SOS was aware of most discrepancies presented in this section of the study prior to writing the letters and thus attempted to deceive Congress and the Georgia General Assembly. After learning of most of these discrepancies in 2022, VoterGA produced a refutation that documented 42 false or deceptive statements in that 10-page SOS letter to legislators.

III. CURRENT VOTING SYSTEM SECURITY ISSUES

1. CURRENT SYSTEM VOTE COUNT FAILURES

a) 2020- Voting system cannot produce correct county results so hand count was certified

In the 2020 Georgia General election, Georgia's Dominion Democracy Suite 5.5 system failed to count the votes accurately in Coffee County. In the original count the system failed to count votes on 40 ballots. After 185 ballots were found just prior to the machine recount, the system failed to count those as well. The Coffee County Board of Elections unanimously voted to certify the hand count as the only accurate total of the election results. The board and others such as VoterGA called for a forensic examination of the server but were ignored.



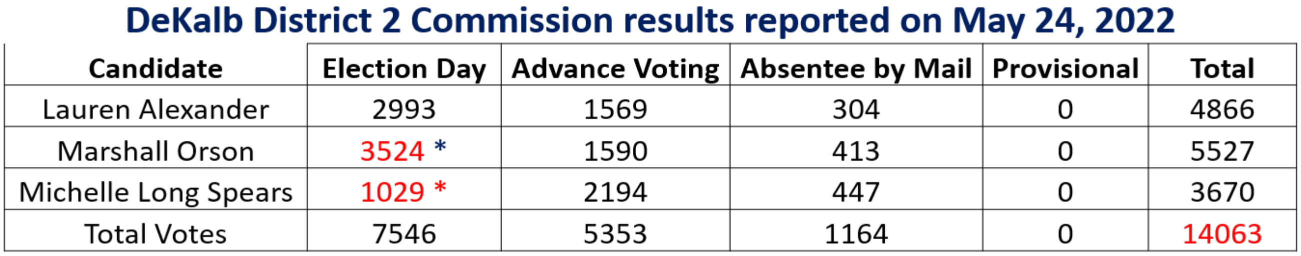
DISCREPENCIES IN THE NOVEMBER 3, 2020 GENERAL ELECTION AND RECOUNTS

Date	Activity	Action #	Trump	Biden	Jorgensen	Write-IN	No Vote*	Total Votes	Internal Delta	Total Delta	Net Discripency Between Total and Internal
11/3/2020	Election Day 1	1	10578	4511	125	23	40	15237			
11/17/2020	Hand Recount	2	10578	4511	126	NA	NA	15238			
	Compare 2 to 1		0	0	+1			+1	+1	+1	0
11/30/2020	Electronic Recount	3	10596	4518	13	0	15	15127			
	Compare 3 to 1		+18	+7	-112			-110	-87	-110	+23
	Compare 3 to 2		+18	+7	-112			-110	-88	-110	+22
11/30/2020	2nd uploaded 185 BALLOTS	4	NO CHANGE	NO CHANGE	NO CHANGE	0	74	NO CHANGE			
	The tabluated Electonic Recount revealed the above discrepencies										
	Investigation revealed we negelected to run 185 balltos: we then ran these ballots										
	we reviewed the resultsbut there was No Change in Vote Count Despite 185 Ballots Added										
	The on Site Dominion Rep could not explain why system would not update votes										
	The Dominion Rep directed the Board of Elections to make a decision about what to do.										
	FOR SOME REASON NO WRITE-IN COLUMN PRINTED ON THE RECOUNT SUMMARY										
	THERE WAS NO EXPLANATION OR SOLUTION TO THIS PROBLEM										
12/2/2020	Prepare to Certify	5	10597	4520	136			15236			
	Compare 5 to 1		+19	+9	+11			-1	+37	+16	+23
	Compare 5 to 2		+19	+9	+11			-2	+38	+16	+24
	There is a discrepency between Electronic Recount and total votes for both 1 & 2										
	Stated Differently after 3 counts a clear inconsistency exists as one compares the orgional election counts, the hand recount, and the electronic recount.										
	Anomilies in software recounts create irreconcilable difference in vote count which leaves the Board with no clear guidance as to which count to certify.										
	*** Write-IN and NO Votes are NOT included in the Total Votes**										

> *"We reviewed the results and there was no change in the vote count despite 185 ballots added."*
>
> Coffee Co. Board of Elections

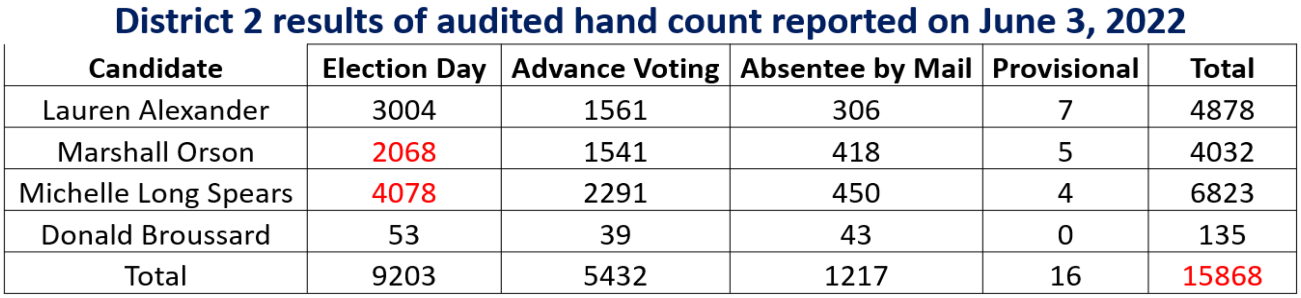
b) 2022- Hand count discovers voting system declares the wrong primary winners

In May of 2022, the Georgia voting system declared the wrong winners in the DeKalb County District 2 Commission Primary. The vote tabulation error was only discovered because a candidate got zero votes in the precinct where she and her family lived and voted. She raised the error to the county election board who conducted a machine recount only to have the same results produced again. They then ordered a hand recount which showed that the candidate had been shorted 3,000 of her 4,000 votes. About 1,400 votes were given to one of her opponents and another 1,800 were not counted at all. While an analysis produced in DeKalb County Election Board Materials for July 14, 2022 attributed the vote transfer to a ballot alignment problem, it fails to explain 1,800 votes were never tabulated.



DeKalb District 2 Commission results reported on May 24, 2022

Candidate	Election Day	Advance Voting	Absentee by Mail	Provisional	Total
Lauren Alexander	2993	1569	304	0	4866
Marshall Orson	3524 *	1590	413	0	5527
Michelle Long Spears	1029 *	2194	447	0	3670
Total Votes	7546	5353	1164	0	14063



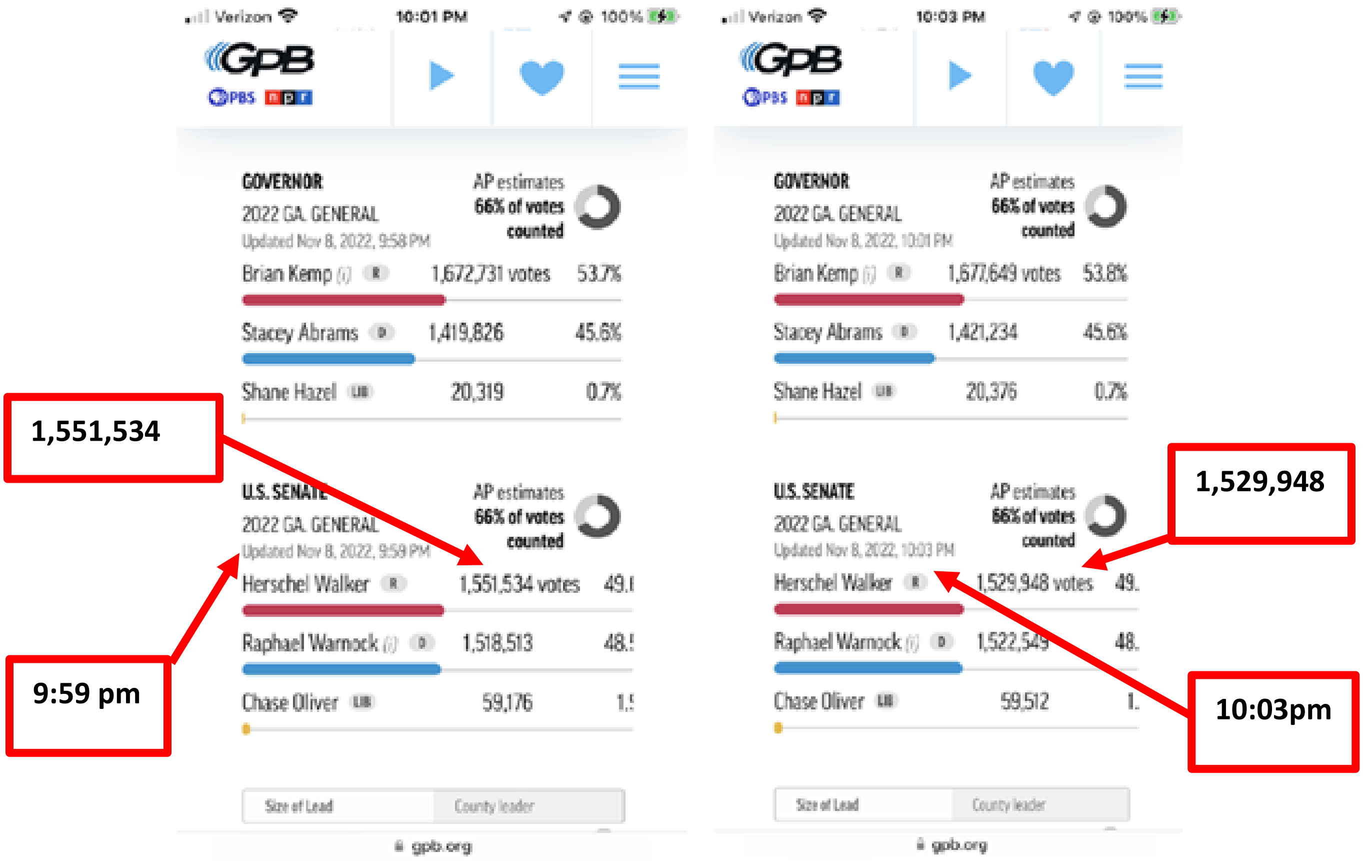
District 2 results of audited hand count reported on June 3, 2022

Candidate	Election Day	Advance Voting	Absentee by Mail	Provisional	Total
Lauren Alexander	3004	1561	306	7	4878
Marshall Orson	2068	1541	418	5	4032
Michelle Long Spears	4078	2291	450	4	6823
Donald Broussard	53	39	43	0	135
Total	9203	5432	1217	16	15868

The county election board was unable to check more races for accuracy because they complained of threats by the SOS office. No other candidate races were fully audited in the primary. That includes the SOS race where Secretary Raffensperger was awarded 51% of the vote to avoid a runoff after polling at 18-39% up until the day of the election. Thus, the Dominion Democracy Suite 5.5 system has a 0% accuracy rate in fully audited 2022 candidate primaries.

c) A 20,000 vote decrease in 4 minutes during 2022 election has fingerprints of cyber attack

In the 2022 U.S. Senate primary, candidate Herschel Walker lost over 21,000 votes in a four-minute span between 9:59 pm and 10:03 pm. At the same time his opponents vote totals increased by over 4,000 and 336 respectively, a technical impossibility. This is illustrated by the Georgia Public Broadcasting election results for that time frame as shown:



Verizon 10:01 PM 100%

GOVERNOR
2022 GA. GENERAL
Updated Nov 8, 2022, 9:58 PM
AP estimates 66% of votes counted

Brian Kemp (i) R	1,672,731 votes	53.7%
Stacey Abrams D	1,419,826	45.6%
Shane Hazel LIB	20,319	0.7%

U.S. SENATE
2022 GA. GENERAL
Updated Nov 8, 2022, 9:59 PM
AP estimates 66% of votes counted

Herschel Walker R	1,551,534 votes	49.
Raphael Warnock (i) D	1,518,513	48.
Chase Oliver LIB	59,176	1.

Size of Lead | County leader

gpb.org

1,551,534

9:59 pm

Verizon 10:03 PM 100%

GOVERNOR
2022 GA. GENERAL
Updated Nov 8, 2022, 10:01 PM
AP estimates 66% of votes counted

Brian Kemp (i) R	1,677,649 votes	53.8%
Stacey Abrams D	1,421,234	45.6%
Shane Hazel LIB	20,376	0.7%

U.S. SENATE
2022 GA. GENERAL
Updated Nov 8, 2022, 10:03 PM
AP estimates 66% of votes counted

Herschel Walker R	1,529,948 votes	49.
Raphael Warnock (i) D	1,522,549	48.
Chase Oliver LIB	59,512	1.

Size of Lead | County leader

gpb.org

1,529,948

10:03pm

The bizarre vote decrease shown also appeared on WSB-TV and the Edison Media line feed. When cross examined under oath, Elections Director Blake Evans could not explain why there would be such a dramatic decrease in votes for one candidate while opposing candidate vote totals continue to increase normally. He further admitted he had been presented the concern but did not investigate it. While this problem could be in the voting system or the Clarity Elections results publishing system, it has the fingerprints of a cyber intrusion.

d) 2022 - Tennessee discontinues Dominion after finding same Georgia QR code error

The SEB 2022-348 case documented that 65 of 67 counties surveyed experienced the “QR Code signature mismatch” error that has been known to cause the system not to tabulate votes on ballots that have been rejected in error. The existence and behavior of this error was confirmed by the Election Assistance Commission (EAC) and Dominion when it was found in Williamson County, Tennessee. The error resulted in votes not being tabulated and caused the SOS to recommend discontinuing use of the Dominion Democracy Suite 5.5 system in Williamson County, which the county did.

This author created two reconciliation rules to ensure that tabulator ballots cast reconcile with scanner counter ballots cast. The SEB approved these rules in 2024 which were never challenged. However, the SOS and the SEB chair never informed counties of the rule change despite three letters I wrote to the SEB Chair.

e) 2024 – The frequency of the QR Code error exceeds maximum allowable federal standards

The QR code error continues to plague Georgia elections. For example, a 2025 Georgians for Truth overview of scanner log files that track scanning processes and errors found: *"A close read of those logs reveals error patterns that raise urgent questions about federal compliance, constitutional requirements, and basic public confidence in how votes are recorded and reported."* This overview summarizes a study of the 2024 Grady County election, which was conducted with no detectable incidents, not only showed the error is still prevalent but it exceeds the maximum allowable federal error standards.

The study analyzed 11 Grady County precinct scanner log files for 10,768 scanned ballots containing about 366,112 ballot positions. Each position represents a single choice on a ballot such as a candidate selection or referendum yes/no vote. The study found 6,317 machine logged errors affecting 58.66% of all ballots cast. Primary error types found included:

- "Ballot has been reversed" — 2,908 instances (46.03% of all errors)
- "Ballot format or ID is unrecognizable" — 1,776 instances (28.11%)
- "Could not find QR code on ballot" — 1,349 instances (21.36%)
- "QR code Signature mismatch" — 284 instances (4.50%)

The 6,317 machine logged errors for 366,112 ballot positions results in a scanner error rate for the 2024 Grady County election of one in 58 ballot positions. Grossly exceeding the limit of one in 10,000,000 ballot positions specified by federal law. 52 U.S.C. § 21081

That law is based on performance standards established by the Federal Election Commission (FEC) in its April 2002, publication entitled *"Voting System Standards Volume 1 – Performance Standards"*. It states *"For each processing function indicated above, the system shall achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions."* [Pg 3-52]

The processing functions include for all paper-based systems: "*Scanning ballot positions on paper ballots to detect selections for individual candidates and contests;"* [3-51]

The study concluded that the actual Grady County 2024 error rate of 1 in nearly 58 ballot positions is over 172,000 more frequent than the maximum allowable federal error rate of 1 in 10,000,000. Studies of the 2024 Georgia election in three other Georgia counties have found similar results.

2. CURRENT VOTING SYSTEM VULNERABILITIES

Most of the vulnerabilities cited in this section are based on September 30, 2024 unrefuted expert witness testimony in the *Dekalb GOP v. Raffensperger* case which is currently the subject of an EAC emergency petition to vacate the certification of Georgia's Dominion Democracy Suite 5.5-A voting system.

a) Georgia's voting system was never legitimately certified by the EAC

Georgia's Dominion Democracy Suite 5.5-A voting system was supposedly certified by the EAC on January 19, 2019. Systems certified by the EAC at that time are required to meet the 2005 Voluntary Voting System Guidelines (VVSG) Volume 1 to obtain federal certification.

According to the 2005 certification guidelines, certified systems must meet Federal Information Processing Standards. These include the 1994 FIPS 140-2 standards for encryption key protection and the 1985 FIPS 112 standards for password security. The next sub sections will show how the unrefuted expert witness testimony revealed that Georgia Dominion Democracy Suite 5.5-A voting system never met these standards despite their age.

Failure to meet voting system standards can easily occur because the EAC uses vendor funded test labs to conduct certification testing. Thus, the testing processing is compromised since test vendors have a vested interest in passing voting systems that are otherwise unqualified to receive certifications.

b) Georgia's voting system cannot meet state certification requirements

To obtain a Georgia state certification, Georgia law requires a voting system to meet federal certification guidelines. It specifically states:

"The state shall furnish a uniform system of electronic ballot markers and ballot scanners for use in each county as soon as possible. Such equipment shall be certified by the United States Election Assistance Commission prior to purchase, lease, or acquisition." O.C.G.A. § 21-2-300(a)(3)

As explained above, Georgia's Dominion voting system never met those guidelines and cannot meet them today. In addition, state certification guidelines require the system to be *"safe for use".* Most any standard definition of the word "use" in this context, implies an ongoing commitment to safety, not simply a one-time event. Therefore, Georgia's voting system simply cannot meet Georgia state certification guidelines for this reason either. Should the certification be vacated by the EAC or otherwise revoked federally, the voting system would be no longer state certified. O.C.G.A. § 21-2-300(a)(2)

c) The voting system's encryption keys are not protected as required for certification

Unrefuted expert witness testimony has shown that Dominion Democracy Suite 5.5-A voting system encryption keys are not secured. FIPS 140-2 standards require encryption keys to be stored in an encrypted module for protection against an intruder. Dominion Democracy Suite 5.5 encryption keys are stored in clear, plain text in a database and thus, do not meet the original standards under which the system was supposedly certified.

FIPS 140-2 standards explain that: *"Plaintext secret and private keys shall not be accessible from outside the cryptographic module to unauthorized operators."* and *"Secret keys, private keys, and CSPs shall be protected within the cryptographic module from unauthorized disclosure, modification, and substitution."*[Pg 30, 33]

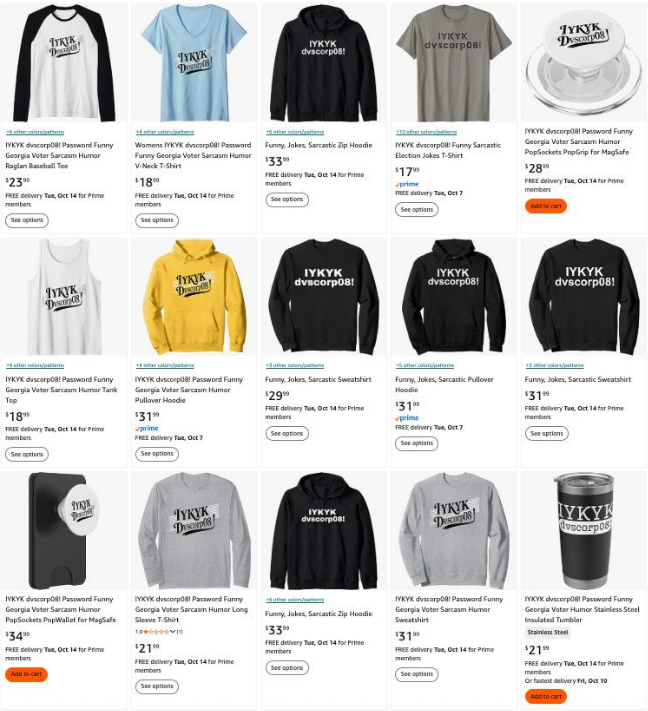
Exposed encryption keys allow a bad actor to retrieve the keys with a simple Structured Query Language (SQL) Select statement. The bad actor can then use standard programs to easily decrypt & change election results and perform many other malicious transactions. Therefore, exposed encryption keys should never be allowed in any voting system.

d) The voting system's password design is not secure enough to meet certification standards

Unrefuted expert witness testimony has shown that the password design for the Dominion Democracy Suite 5.5-A voting system is fatally flawed. The voting system was delivered with a hard coded administrative account password that was never changed.

FIPS 112 standards require that: "Passwords shall have a maximum lifetime of 1 year." and "*All passwords that may be included in a new system when it is delivered, transferred or installed ….shall be immediately changed by the Security Officer.*" Pg 11

A password should never be hard coded because once known, there is no means to protect administrative functions from being nefariously performed. The administrative password is now publicly known and available on a variety of apparel items as shown below:



+6 other colors/patterns
IYKYK dvscorp08! Password Funny Georgia Voter Sarcasm Humor Raglan Baseball Tee
$23.99
FREE delivery **Tue, Oct 14** for Prime members
See options

+4 other colors/patterns
Womens IYKYK dvscorp08! Password Funny Georgia Voter Sarcasm Humor V-Neck T-Shirt
$18.99
FREE delivery **Tue, Oct 14** for Prime members
See options

+6 other colors/patterns
Funny, Jokes, Sarcastic Zip Hoodie
$33.99
FREE delivery **Tue, Oct 14** for Prime members
See options

+10 other colors/patterns
IYKYK dvscorp08! Funny Sarcastic Election Jokes T-Shirt
$17.99
✓prime
FREE delivery **Tue, Oct 7**
See options

IYKYK dvscorp08! Password Funny Georgia Voter Sarcasm Humor PopSockets PopGrip for MagSafe
$28.99
FREE delivery **Tue, Oct 14** for Prime members
Add to cart

+4 other colors/patterns
IYKYK dvscorp08! Password Funny Georgia Voter Sarcasm Humor Tank Top
$18.99
FREE delivery **Tue, Oct 14** for Prime members
See options

+4 other colors/patterns
IYKYK dvscorp08! Password Funny Georgia Voter Sarcasm Humor Pullover Hoodie
$31.99
✓prime
FREE delivery **Tue, Oct 7**
See options

+3 other colors/patterns
Funny, Jokes, Sarcastic Sweatshirt
$29.99
FREE delivery **Tue, Oct 14** for Prime members
See options

+5 other colors/patterns
Funny, Jokes, Sarcastic Pullover Hoodie
$31.99
✓prime
FREE delivery **Tue, Oct 7**
See options

+3 other colors/patterns
Funny, Jokes, Sarcastic Sweatshirt
$31.99
FREE delivery **Tue, Oct 14** for Prime members
See options

IYKYK dvscorp08! Password Funny Georgia Voter Sarcasm Humor PopSockets PopWallet for MagSafe
$34.99
FREE delivery **Tue, Oct 14** for Prime members
Add to cart

IYKYK dvscorp08! Password Funny Georgia Voter Sarcasm Humor Long Sleeve T-Shirt
1.0 ★☆☆☆☆ (1)
$21.99
FREE delivery **Tue, Oct 14** for Prime members
See options

+6 other colors/patterns
Funny, Jokes, Sarcastic Zip Hoodie
$33.99
FREE delivery **Tue, Oct 14** for Prime members
See options

IYKYK dvscorp08! Password Funny Georgia Voter Sarcasm Humor Sweatshirt
$31.99
FREE delivery **Tue, Oct 14** for Prime members
See options

IYKYK dvscorp08! Password Funny Georgia Voter Humor Stainless Steel Insulated Tumbler
Stainless Steel
$21.99
FREE delivery **Tue, Oct 14** for Prime members
Or fastest delivery **Fri, Oct 10**
Add to cart

Dominion passwords are also not irreversibly hashed as most passwords are but instead, they are encrypted. With the encryption key exposure previously described, the passwords can easily be retrieved, decrypted and used for nefarious transactions.

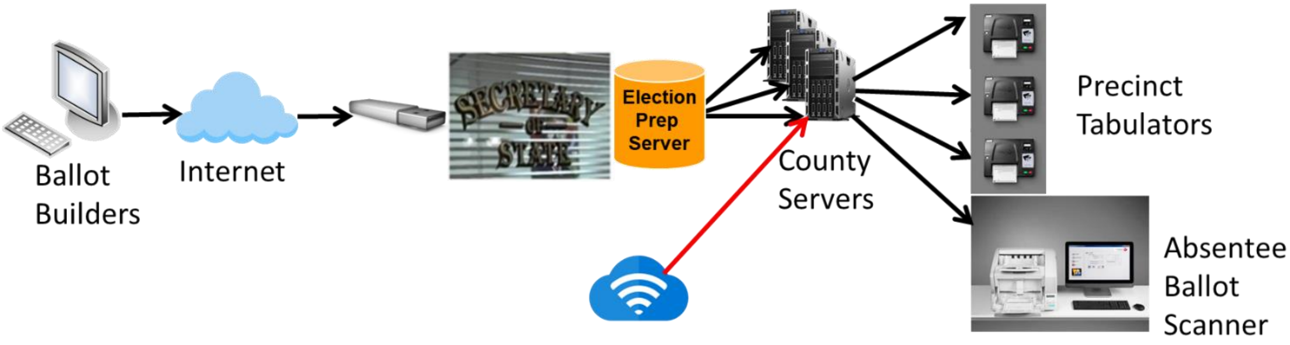
Furthermore, the passwords are generic instead of specific to individual users. If users are sharing a generic password to make database updates there is no means to track a specific update back to the user who performed the update transaction.

e) Georgia's voting system components are configured for remote connectivity

Unrefuted expert witness testimony has shown that all Dominion Democracy Suite 5 voting systems can communicate with each other worldwide via a **common shared value** in an X.509 certificate. While it may be normal to use an X.509 certificate, it is highly irregular for every installation across the world to have the same shared value which essentially serves as a common password throughout the voting system network.

In addition, a forensic study produced by cybersecurity expert Ben Cotton, a highly credentialed cyber forensics specialist, for a Georgia 2020 Election Management Server (EMS) showed that the internet had been accessed after the server installation in 2019. The Georgia study is further corroborated by a Colorado Dominion Democracy Suite 5.11 forensic study showing all key components of the server are configured to be remotely accessed. That study showed the voting system database is configured to allow remote access, well known default ports are used, there are no firewall rules to prevent outside intruders from accessing the server and an uncertified SQL Server Management Studio (SSMS) tool is also configured for remote access.

This dangerous configuration allows someone with access to a Dominion Democracy Suite system to access any other Dominion Democracy Suite voting system from anywhere in the world as shown:



Unauthorized and undetected remote accessibility is obviously a grave concern. The EAC's Technical Development Guidelines Committee. (TDGC) sought to ban remote accessibility from all voting systems in 2021. When the EAC Commissioners resisted, Dr. Stark, then head of the TDGC committee, filed a lawsuit against the EAC.

f) Georgia's Dominion voting system was programmed remotely by Serbians

A trove of Email discovery produced in the *Dominion v. Byrne* case and released by Michigan Sheriff Dar Leaf in a letter to Judiciary Committee Chairman Jim Jordan indicate Dominion Voting Systems have been programmed and maintained from Belgrade, Serbia. Dominion even experienced unknown logins from Kosovo. Emails specifically show that the 2020 Gwinnett County server package was produced by a Serbian program team operating outside of the U.S. It is interesting to note that this same server experienced a malfunction in the 2020 General Election where the Gwinnett voting system failed to count Presidential votes on 1,642 ballots.

g) Georgia's voting system has been maintained and accessed remotely by Serbians

Another Email discovered shows evidence that Georgia's Dominion Democracy Suite 5.5-A is maintained remotely by Serbians. The Serbian programmers attempted to resolve a deadlock issue during the 2020 Primary Runoffs. This issue was also experienced in Dominion systems running in Michigan and Colorado.

The Belgrade office was reportedly shut down recently within weeks after the acquisition by Liberty Vote. **This foreign involvement and remote access in U.S. elections, including those in Georgia, was withheld by the SOS and denied when Dominion CEO John Polous testified to the Michigan legislative committee and the Georgia SEB.**

h) Dominion accessed a Georgia county server remotely during the 2021 U.S. Senate runoff

As previously explained, the Coffee County voting system failed to count votes on 40 ballots during the original machine count and ignored 185 more during the machine recount. The election board unanimously voted to certify the hand count as the only accurate total of the election results. They, VoterGA and others called for a forensic examination of the server but were ignored by the SOS.

On December 10, 2020, a board member testified before the House Government Affairs Committee and turned over 13 MB of material to document the tabulation problems. On the same day, then SOS legal counsel Ryan Germany wrote to the lead SOS investigator claiming that the board member lied about not getting SOS help and asked the investigator to talk with him while she was down there. The investigator, who has virtually no technical background, testified in January 2024 that she concluded the tabulation problem was caused by not separating batches correctly, a technical impossibility given the circumstances.

In the 2021 U.S. Senate race, Coffee County again experienced similar absentee ballot rejection problems causing board members and election workers to become frustrated with on-site Dominion technical support personnel who were unable to solve the problem. Depositions and a referenced affidavit show that after a 30-minute private phone conversation outside of the office, a Dominion worker returned stating he had a solution, held his cellphone near the Election Management Server (EMS) and corrected the absentee ballot rejection problem without touching any equipment, including the EMS and absentee ballot scanner. The Elections Director and another witness realized they had watched their system be remotely patched.

After getting **no** help from the SOS office again in obtaining a forensic examination of the system, election board members decided to arrange for a professional chain of custody firm to take a software image copy of the server and other components for forensic examination. A copy does not change any data on any component. The copy was then placed on a secure site and a key to the site was given to an election attorney. That attorney engaged cybersecurity expert, Ben Cotton, to forensically examine the server and conduct a security assessment of the system. Mr. Cotton found extensive evidence of remote connectivity, undetected election program manipulation and a dynamic malware compiling capability.

The elections staff also allowed another expert, Jeffrey Lenberg, to instruct the Election Director on tests that could be made to determine what was changed. Mr. Lenberg is a nation-state vulnerability testing expert with 30 years of experience at Sandia National Labs. Based on the tests the director performed without impacting the system operation in any way, he was able to determine the exact configuration parameter Dominion accessed and setting that was changed to stop ballot rejections without touching the system. This stunning discovery is documented in his deposition.

i) Over 3,000 county election server program files were modified after its 2020 installation

The forensic study of an authenticated copy of a Georgia 2020 EMS and expert witness testimony from Ben Cotton showed that the server had **over 3,000 EMS server program files that were secretly modified** after its installation in 2020. Such drastic modifications of program files could not have been done manually and would surely have invalidated the certification if the modifications had been detected. This evidence, when revealed in court, should have warranted an immediate public investigation of all county voting systems by the SOS.

j) The server's uncertified compiler allows malware to be created and distributed remotely

The forensic study on an authenticated copy of a 2020 Georgia county EMS and expert witness testimony from Ben Cotton further showed the EMS contained an uncertified compiler that can allow malware to be created and spread to nearly all key county voting system components. A compiler accepts programmer instructions dynamically and converts them into machine code. Anyone with access can write or compile any type of program or malware to rig elections and deploy it to all county voting system components undetected. The known presence of a compiler should have warranted an immediate discontinuance of the system by the SOS.

k) An authenticated copy of a Georgia county server was hacked in 3-minute court demo

The uncertified SSMS data manipulation tool can be used to bypass Dominion software and allow anyone to manipulate the election database by easily decrypting results, flipping votes, encrypting the new results and updating the database. Just such a manipulation was demonstrated in September 2024 testimony by expert witness Clay Parikh, a cybersecurity expert and voting system tester with experience in 7 different voting systems. He demonstrated in Fulton Superior Court how to hack an authenticated copy of a Georgia county EMS. Mr. Parikh changed the results of the Presidential race in a 3-minute demonstration using only 6 lines of stored procedure code.

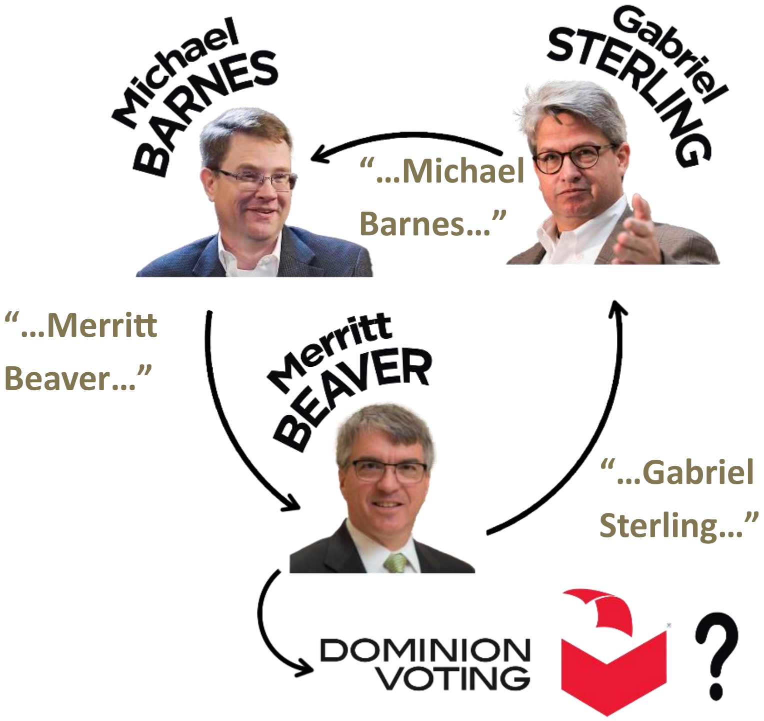
l) No one in the SOS office is responsible for cyber security

During the January 2024 *Curling v. Raffensperger* trial, Plaintiff Ricardo Davis attempted to determine who was responsible for cyber security in the SOS office. Gabriel Sterling replied that" *"It falls to Michael Barnes and his team for the physical security, as well as the cybersecurity with the IT team."* 1-17-24 Vol 6a, 12:20-13-25.

When Michael Barnes took the stand, he explained he has no direct responsibility for cyber security and added: *"The people that maintain for the Secretary of State's office their infrastructure security measures are the Secretary of State's IT division". "Merritt Beaver has been our CIO".* 1-17-24 Vol 6a, 12:20-13-25.

When Chief Information Officer Merritt Beaver testified that: "Dominion did not report to me." and "Gabe Sterling" had the higher authority for cyber security. He also added: *"We outsource the security for the Dominion system to Dominion."* 1-16-24 Vol 5A, 105:6-113:1.

Dominion cannot provide cyber security protection for the SOS office. It is obvious from this vicious circle that no one in the office is responsible for cyber security.



3. FEDERAL AND STATE COMPLIANCE ISSUES

a) The U.S. District Court found in Oct. 2020 that Georgia's voting system violates two statues

As previously explained, the U.S. District Court found in October 2020 that the QR coded vote tabulation system violates two Georgia statutes for verifiability and elector readable choices. Nevertheless, the November 2020 Georgia General Election was conducted on a voting system that the U.S. District Court found violates Georgia laws and continues to violate Georgia laws. O.C.G.A. § § 21-2-2(7.1), 21-2-300(a)(2)

b) The Georgia General Assembly more explicitly outlawed QR code vote tabulation

After the SOS failed to act on the U.S. District Court rulings, the Georgia General Assembly even more explicitly banned the QR code vote tabulation effective with SB189, which was signed into law as Act 697 by Governor Kemp on May 6, 2024, with an effective date of July 1, 2026. The code addition reads:

"The official tabulation count of any ballot scanner shall be based upon the text portion or the machine mark, provided that such mark clearly denotes the elector's selection and does not use a QR code, bar code, or similar coding, of such ballots and not any machine coding that may be printed on such ballots." (O.C.G.A. § 21-2-379.23)

But that is only one of several more federal and state legal compliance issues that Georgia's voting system is facing.

c) The voting system cannot meet HAVA voter verifiability standards

The U.S. Help America Vote Act (HAVA) requires voting systems to: *"(i) permit the voter to verify … the votes selected by the voter on the ballot before the ballot is cast and counted;"* Title 3 Sec. 301 (1) (A) (i)

The votes allegedly selected by the voter are shown in text by Georgia's voting system to voters but the votes it accumulates are hidden in a QR code that the voter cannot verify. It is disingenuous to claim that a QR coded vote tabulation can comply with federal HAVA verifiability law.

d) The EAC is decertifying all QR code vote tabulation systems per Executive Order

Section 4 (b) (i) and (ii) of Executive Order (EO) 14248, Preserving and Protecting the Integrity of American Elections, which was signed on March 25, 2025, order the EAC to update certification guidelines to explicitly ban unverifiable QR code vote tabulation while decertifying all previous voting systems. The applicable paragraphs read:

- *'(b)(i) The Election Assistance Commission shall initiate appropriate action to amend the Voluntary Voting System Guidelines 2.0 and issue other appropriate guidance establishing standards for voting systems to protect election integrity. The amended guidelines and other guidance shall provide that voting systems should not use a ballot in which a vote is contained within a barcode or quick-response code in the vote counting process except where necessary to accommodate individuals with disabilities, and should provide a voter-verifiable paper record to prevent fraud or mistake.*

- *(ii) Within 180 days of the date of this order, the Election Assistance Commission shall take appropriate action to review and, if appropriate, re-certify voting systems under the new standards established under subsection (b)(i) of this section, and to rescind all previous certifications of voting equipment based on prior standards."*

Georgia's Dominion Democracy Suite 5.5-A voting system must be comprehensively modified to eliminate unverifiable QR code vote tabulation for in-person voters. In addition, the system is faced with a previously explained encryption key exposure problem that renders it uncertifiable under 2005 EAC guidelines and FIPS 140-2 security standards. This deficiency requires yet another set of major enhancements before it could even be presented to the EAC for re-certification. Once completed the system is faced with a lengthy re-certification process just to prove it has solved these two problems. Such changes are yet to be completed, if they are in progress. Consequently, no such re-certification process is underway further rendering the system uncertifiable for the 2026 election.

e) Georgia's voting system cannot meet federal critical infrastructure certification standards

Another problem complicating the Dominion Democracy Suite 5 certification process, is that it cannot meet federal critical infrastructure standards under which voting systems must comply. On January 6, 2017, just before leaving office, President Obama's Department of Homeland Security (DHS) Secretary Jeh Johnson designated election systems as critical infrastructure. This action taken to secure federal elections imposes new constraints upon voting system vendors. 42 U.S.C. 5195c(e)

Georgia's foreign owned voting system was produced by a Canadian based holding company with unspecified international investors. It is programmed and maintained remotely by Serbians, has manufactured components shipped from China and runs on servers using programmable Chinese chipsets which include server motherboards as revealed in Sheriff Dar Leaf's letter to Jim Jordan. All of this is noncompliant with federal requirements for critical infrastructure such as the Defense Production Act (DPA) and the Federal Information System Modernization Act (FISMA).

While many believe that the Constitution requires only states to run elections, the second sentence of Art. I Sec. IV of U.S. Constitution clearly provides Congress with authority to ultimately decide most federal election issues. It reads:

"The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Place of Chusing [sp.] Senators"

This Constitutional clause authorized federal election laws like HAVA, the National Voter Registration Act and the National Voting Rights Act. Furthermore, the President has power to enforce federal laws under Art. II, Sec. III, of the Constitution in that *"…he shall take Care that the Laws be faithfully executed."*

As we come to the realization that we have a national security crisis in elections, we should also keep in mind that Presidents have enforcement power under National Emergencies Act. Therefore, any new system Georgia may consider for 2026 must be fully compliant with federal law to conduct federal elections.

f) The GA Supreme Court ruled that paper ballot and hand count statutes apply to BMDs

In October 2020, the Georgia Supreme Court ruled that paper ballot statutes apply to Georgia's BMD elections. *Rhoden v. Athens-Clarke County BoE* 310 Ga. 266 (2020). The ruling explicitly cited O.C.G.A. § 21-2-437. This statute requires hand marked paper ballots and hand counting. It reads:

- *"Any ballot marked by anything but pen or pencil shall be void and not counted…"*

The statute also has extensive provisions mandating a hand counting of ballots at the precinct. For example, it states:

- *"The ballots shall then be counted one by one and a record made of the total number"*

These procedures are not currently being followed by Georgia elections. A hand marked paper ballot, hand counted solution, as the Georgia Supreme Court advocated, would eliminate all legal and certification issues facing Georgia for 2026.

g) A pending emergency EAC petition could soon vacate Georgia's voting system certification

An emergency EAC petition was filed on October 24, 2025, to vacate Georgia's Dominion Democracy Suite 5.5-A certification. The previous sub sections explain how it did not comply, and does not comply, with 2005 EAC certification guidelines that prohibit exposed encryption keys and hard coded passwords. Hard coded passwords and cryptographic keys were known deficiencies of the Dominion Democracy Suite 4.0 system as identified in the Wyle Test Deficiency Report. This illustrates a lack of concern in resolving deficiencies.

Experts further testified that all Dominion Democracy Suite 5 systems have the same security flaws. Other petitioners or petitioner groups from additional states have joined the petition or submitted their own similar petitions further increasing pressure on the EAC to act. Should the EAC uphold the petition, or petitioners prevail in a U.S. District court emergency action, the voting system could lose its federal certification. Such a loss would also likely result in the system losing its state certification since state law requires that any Georgia voting system used be certified by the EAC.

h) Compliant security protections cannot practically be retrofitted into Georgia's voting system

The security compliance issues cited in this study for Georgia's Dominion Democracy Suite 5.5-A system are overwhelming and present a severe dilemma for Georgia voters and election officials. There is no known, provable software patch that can safely resolve them.

Dr. Alex Halderman found in his U.S. District Court Security Analysis that Georgia's BMD system *"… was developed without sufficient attention to security during design, software engineering, and testing."* He concluded: *"…it would be extremely difficult to retrofit security into a system that was not initially produced with such a process."*

This extensive security deficiency in Georgia's Dominion Democracy Suite 5.5-A voting system precludes a lack of any practical, genuine, remediation alternatives. This unresolvable nature of these overwhelming security deficiencies. renders the system not usable for the 2026 election cycle.

IV. CURRENT VOTER DATA SECURITY ISSUES

1. CLOUD BASED VOTER REGISTRATION DATA THREATS

a) The SOS moved voter registration system to a cloud without consent of the legislature

Georgia law requires the SOS to maintain the official list of electors (voters) in this state. There is no provision in Georgia law for a third party to do so. The enabling statute, O.C.G.A § 21-2-211, explicitly states:

- *"(a) The Secretary of State shall establish and maintain a list of all eligible and qualified registered electors in this state which shall be the official list of electors for use in all elections in this state conducted under this title."*

The enabling statute also placed restrictions on funding:

- *(b)(2) The Secretary of State is authorized to procure and provide all of the necessary equipment to permit the county boards of registrars to access and utilize the official list of electors maintained by the Secretary of State pursuant to this Code section, provided that funds are specifically appropriated by the General Assembly for that purpose.*

No funds were appropriated for the express purpose of outsourcing voter registration data to a cloud.

On January 19, 2022, the SOS announced outsourcing of our voter data that occurred via a no-bid $3.5 million contract although bids should have been obtained on values over $100,000. The contract bid restrictions were circumvented through what was essentially a Carahsoft blanket purchase order.

Outsourcing private portions of our Voter registration data further conflicts with the voter data privacy statute, O.C.G.A. § 21-225.1, which requires board of registrars *"…to make such elector's residence address confidential"* under certain circumstances.

- *"(d) The Secretary of State shall provide by procedure, rule, or regulation for the mechanism by which such information shall be made confidential on the voter registration data base and may provide for forms for use in making such requests and for the use of alternate addresses for electors who file requests for the confidentiality of their residence addresses."*

There is no mechanism to ensure an elector's address can remain confidential if it has been outsourced and to a 3rd party.

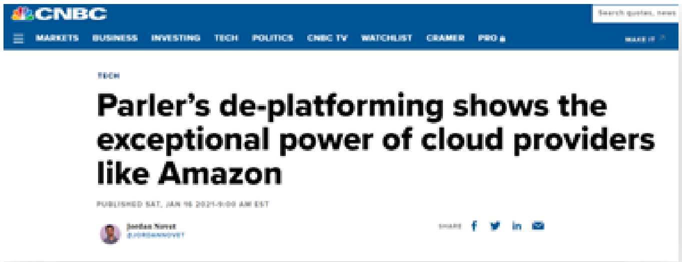
b) The GARVIS cloud-based voter registration eliminates SOS control of voter registration data

Prior to the recent outsourcing of Georgia's voter registration database, the SOS had complete direct control of the voter registration database and system. Although vendor products were employed, the products were used to form a total in-house solution for voter registration and the voter registration database.

Nevertheless, the SOS decided to contract with Salesforce, a popular Customer Relationship Management system vendor. Its cloud platform is not really suitable for a mission critical system such Voter Registration as explained in the following sub sections. Despite a still active, March 10, 2022 pending lawsuit against outsourcing, the SOS continued with the cloud-based implementation, ignored the following risks described and implemented a cloud-based voter registration system now known as GARVIS.

c) Third party service providers can de-platform Georgia's voter registration system anytime

Salesforce relies on Amazon Web Services for key voter registration transactions. Amazon Web Services abruptly de-platformed the Parler social media platform just as it was becoming a leading conservative based alternative to Facebook and other social media platforms. Amazon's abrupt, politically motivated discontinuance of Parler essentially destroyed their growth and Parler, then faced with re-writing their entire application, was never able to fully recover.



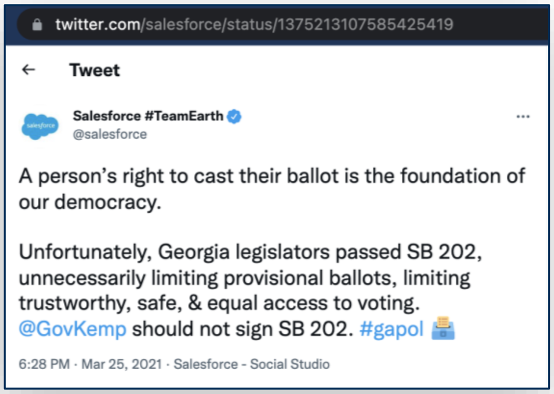
TECH

Parler's de-platforming shows the exceptional power of cloud providers like Amazon

PUBLISHED SAT, JAN 16 2021-9:00 AM EST

Jordan Novet
@JORDANNOVET

Amazon or Salesforce could decide at any time to de-platform the entire Georgia voter registration system or impose uncontrollable subscription pricing due to their adversarial nature against Georgia. Salesforce and its CEO Marc Benioff, a World Economic Forum Trustee, already gave notice of their adversarial stances before the Georgia acquisition took place. Although both are California based, Salesforce and Mr. Benioff publicly attacked legislators over the passage of SB202 (and its sister bill HB531) claiming in March 2021 that: *"Unfortunately, Georgia legislators passed SB202, unnecessarily limiting provisional ballots, limiting trustworthy, safe, & equal access to voting".*

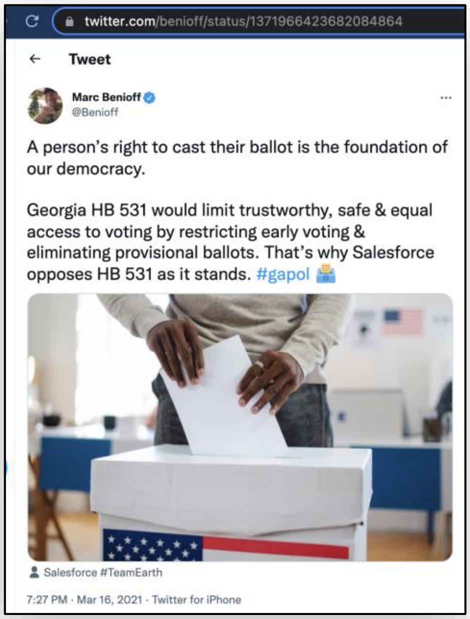


Salesforce #TeamEarth
@salesforce

A person's right to cast their ballot is the foundation of our democracy.

Unfortunately, Georgia legislators passed SB 202, unnecessarily limiting provisional ballots, limiting trustworthy, safe, & equal access to voting. @GovKemp should not sign SB 202. #gapol 🗳

6:28 PM · Mar 25, 2021 · Salesforce - Social Studio



Marc Benioff
@Benioff

A person's right to cast their ballot is the foundation of our democracy.

Georgia HB 531 would limit trustworthy, safe & equal access to voting by restricting early voting & eliminating provisional ballots. That's why Salesforce opposes HB 531 as it stands. #gapol 🗳

Salesforce #TeamEarth

7:27 PM · Mar 16, 2021 · Twitter for iPhone

d) Cloud based voter registration is vulnerable to massive, extreme security risks

Outsourcing Georgia's voter registration database and application functions to a cloud, exposes both the voter registration data and voter registration system functions to overwhelming, extreme security risks when compared to the previous in-house system. These risks include:

- **Application integration risks** – Integration between in-house voter registration applications and the outsourced cloud services can be intercepted by hackers and misdirected for nefarious purposes;

- **Unauthorized function risks** – Authorizations of voter data creation, reads, updates and deletes are not performed on the cloud server but instead left open to errors by developers on the client side;
- **Ease of User Impersonation** – Hackers can more easily impersonate election officials remotely while in the cloud when they would otherwise have no access to a privately secure in-house system;
- **Misconfiguration Risks** - If an instance is misconfigured, a hacker can hijack voter data update sessions and upload malicious content or exploit weaknesses in settings and encryption keys;
- **Cross Site Scripting** – Hackers can hijack scripts in pages of the web-based voter data interface and embed instructions to perform malicious activities that continually corrupt voter data;
- **SQL Injection** – Hackers can use characters in a voter data input form to modify resulting database queries (Salesforce Object Query Language is derivative of standard Structured Query Language)

e) Salesforce was sued for security breaches and not informing their customers about them

Before Georgia's contract signing, Salesforce was cited in a class action lawsuit by customers of a national children's apparel retailer after its platform became infected with malware. The retailer, Hanna Andersson, used the Salesforce platform for its customer data which was obtained by hackers. The malware acquired Personal Identifying Information (PII) of about 20,000 customers that *"was stolen from Hanna's website by unknown individuals, then sold on the dark web."*

The lawsuit claims: *"they stole customers' billing and shipping addresses, payment card numbers, CVV codes, and credit card expiration dates. The criminals got everything they needed to illegally use Hanna's customers' credit cards to make fraudulent purchases, and to steal the customers' identities."*

The lawsuit also alleges that: *"Salesforce failed to detect the breach for almost three months"* and they only learned of it because "*law enforcement found the stolen information on the dark web and warned Hanna".* "Hanna then investigated the breach, confirmed that Salesforce Commerce Cloud's ecommerce platform *was "infected with malware,"*.

The lawsuit further points to a Salesforce coverup: *"Salesforce has not released a vulnerabilities and exposures report, nor has Salesforce made any notifications of the breach".*

f) A Georgia election was disrupted by other Salesforce customer shared resource shortages

The outsourcing of the Georgia voter registration system into a cloud forced Georgia to share cloud-based resources with other Salesforce customers. These resources proved to be not scalable enough to handle the peak demand of an election. As a result, Georgia voters experienced a critical five hour voting outage from about 11am to 4pm on Election Day during the May 21, 2024 primary as acknowledged by Gabriel Sterling.

The Election Day outage made voter data on Georgia's My Voter Page inaccessible to all voters attempting to locate their precincts and other voter information. It also prevented all county election offices from verifying voters who turned in their absentee ballots there and from updating receipt of mail-in ballots to prevent double voting. The outage did not affect most voters since precinct voter lists are downloaded to each poll pad in advance for Election Day voter verification. However, with a new attempt to put Election Day poll books on-line, the risk of an outage will likely increase for the 2026 election.

g) The voter registration system was implemented mostly by inexperienced non-U.S. citizens

The chosen GARVIS implementer, Texas-based MTX, had no election system experience, poor performance on a Texas no-bid contract and only three employees in America when Georgia's contract was signed. MTX outsourced programming to its India-based staff who are not U.S. citizens and were not sworn to uphold the U.S. Constitution.

Prior to being engaged in Georgia, MTX had received severe negative criticism over a Texas medical system. The Houston Chronicle reported *"MTX workers are using their own computers and personal email addresses, fueling worries — unwarranted worries, the state says — that private medical information about the people they investigate could be inadvertently divulged."* State Rep. Donna Howard of Austin, a longtime House Appropriations Committee member, said: *"I'm especially concerned because it is so critical that we have this in place and it's just been one fumble after another. "*

h) The GARVIS implementation resulted in a year-long delay and over 3500 support tickets

The GARVIS system was announced as development complete on January 19, 2022, and scheduled for a March 9, 2022 launch that had to be delayed a year until March 2023. The SOS office claimed the November, 2023 municipal elections were "successful' despite GARVIS having over 3,500 open support tickets that year and having to freeze defect corrections until December. The 2024 primaries were the first time the system was used in a statewide election.

The system has not functioned correctly since its implementation. Election directors and board members have repeatedly criticized the system and some have requested the SOS office return to the more secure ENet system.

2. UNSECURED VOTER AND DRIVER PRIVACY

a) The ERIC agreement compromises the security of Georgians PII in several ways

On May 22, 2019, the SOS announced an agreement to have the state of Georgia join the Electronic Registration and Information Center (ERIC). The one-sided agreement committed Georgia to transfer Georgians PII to ERIC under the pretext of helping to maintain Georgia voter rolls. The Executive Director of ERIC, Shane Hamlin, told the committee that ERIC houses the data in a secret out of state location he refused to disclosed. The transfer of Georgians' PII to any non-governmental 3rd party compromises the security of that PII. It also conflicts with the clear, plain text of federal law and the published understanding of the agreement that the Georgia Department of Driver Services (DDS) has with the SOS and Georgia drivers. All of this is explained in the following subsections.

b) Transmission of Voter PII to ERIC without consent presents legal and security issues

The ERIC member agreement, shown as Exhibit A of the bylaws, requires states like Georgia to send ERIC the Personal Identifying Information (PII) for all Georgia voters without their knowledge or consent. The PII includes data such as Drivers' License ID, last 4 of Social Security Number (SSN), plus Phone number and Email address. In addition, the elector's address is transferred despite the fact that O.C.G.A. § 21-2-225.1 requires boards of registrars *"…to make such elector's residence address confidential"* under certain circumstances. The elector's address cannot be maintained as confidential if it is transferred to a third party that must access it for testing purposes and to support production retrievals and updates.

c) Transmission of driver PII to ERIC without consent conflicts with privacy protection law

The ERIC member agreement also blazingly requires that: *"the Member shall transmit … (2) all licensing identification records contained in the motor vehicles database…"* to ERIC. The transfer may include PII for Georgia non-citizens, teens who have drivers' licenses but are too young to vote, those who chose not to register to vote and others. The transfer not only jeopardizes the security of Georgia driver PII, it also unnecessarily appears to conflict with the federal Driver Protection Act that provides:

- *"A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity:*
  - *(1) personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, …*
  - *(2) highly restricted personal information, as defined in 18 U.S.C. 2725(4), about any individual obtained by the department in connection with a motor vehicle record, without the express consent of the person to whom such information applies…"* 18 U.S.C. § 2721.

Driver data is clearly not needed for voter roll maintenance and should have never been unnecessarily transferred to a 3rd party.

d) ERIC Executive Director claims that ERIC hashes PII are contradicted by his testimony

Mr. Hamlin told the study committee that Georgians' PII is stored in a secret location he refused to disclose. This also appears to violate federal driver privacy law. He admitted that ERIC three employees access the data remotely through their home network via a Virtual Private Network (VPN).

Mr. Hamlin claimed that PII transferred from Georgia to ERIC is hashed. A hash is an algorithm that irreversibly transforms data of any size into a unique fixed size hash value. The hash algorithm can be run on a copy of the original data and the hash values can be compared to ensure a copy is authentic. Hashes are typically standard, publicly available routines such as the National Institute of Standards (NIST) Secure Hash Algorithm (SHA) that Dominion uses to authenticate ballot images.

The claim that ERIC hashes PII it receives is contradicted in several ways by Mr. Hamlin's own testimony:

- First, as Mr. Evans and Mr. Hamlin explained, ERIC uses a proprietary coding routine, not an industry standard hash algorithm;
- Second, Mr. Hamlin acknowledges that a true hash is irreversible;
- Third, Mr. Hamlin admitted that ERIC transferred Georgia data to CEIR and Emails show that they processed it, thus it could have never been irreversibly hashed.

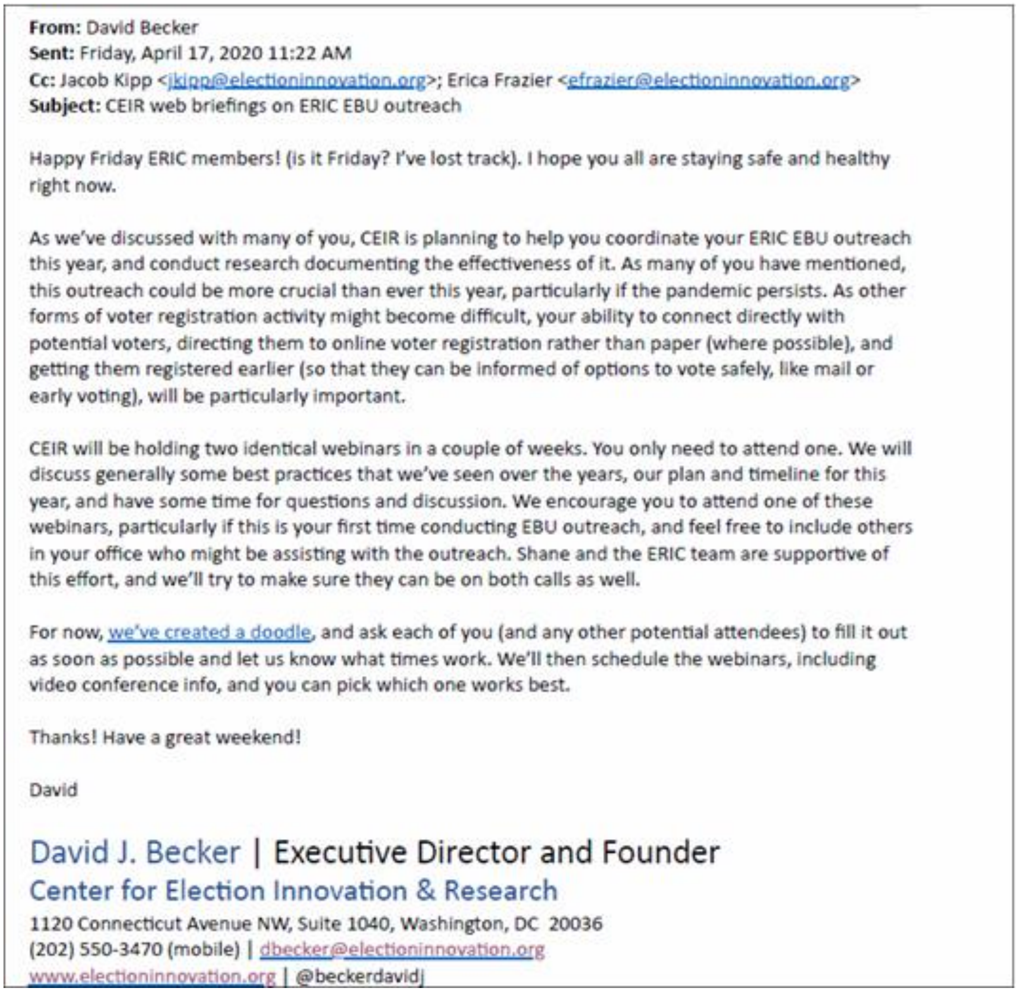
It is simply not possible that ERIC could hash Georgia data that they transferred to CEIR. Therefore, Georgia data transferred to ERIC, is in yet another way, unsecure.

e) The ERIC member agreement imposes unnecessary and undesirable constraints on Georgia

The ERIC member agreement imposes unnecessary and undesirable activities on Georgia such as requiring the state to contact eligible but unregistered Georgians in an attempt to register them to vote. Get out the vote efforts are not the responsibility of the SOS. The SOS should have focused on running safe and secure elections that prevent the problems documented in this study from occurring. While ERIC supposedly granted Georgia a waiver on this requirement, they could rescind the waiver at any time. Georgia has no such protection against a recension and should have never subordinated their elections to a 3rd party in the first place.

f) ERIC transferred Georgian's PII to CEIR, a partisan organization founded by David Becker

Mr. Hamlin acknowledged to the committee that ERIC transferred data they received from Georgia to the Center for Election Innovation and Research (CEIR). The founder of both organizations is David Becker. The following Email from Mr. Becker confirmed that ERIC coordinated this effort which conflicts with the clear, plain text of both the federal Driver Protection Act and the memo of understanding (MOU) between the SOS and DDS.



From: David Becker
Sent: Friday, April 17, 2020 11:22 AM
Cc: Jacob Kipp <jkipp@electioninnovation.org>; Erica Frazier <efrazier@electioninnovation.org>
Subject: CEIR web briefings on ERIC EBU outreach

Happy Friday ERIC members! (is it Friday? I've lost track). I hope you all are staying safe and healthy right now.

As we've discussed with many of you, CEIR is planning to help you coordinate your ERIC EBU outreach this year, and conduct research documenting the effectiveness of it. As many of you have mentioned, this outreach could be more crucial than ever this year, particularly if the pandemic persists. As other forms of voter registration activity might become difficult, your ability to connect directly with potential voters, directing them to online voter registration rather than paper (where possible), and getting them registered earlier (so that they can be informed of options to vote safely, like mail or early voting), will be particularly important.

CEIR will be holding two identical webinars in a couple of weeks. You only need to attend one. We will discuss generally some best practices that we've seen over the years, our plan and timeline for this year, and have some time for questions and discussion. We encourage you to attend one of these webinars, particularly if this is your first time conducting EBU outreach, and feel free to include others in your office who might be assisting with the outreach. Shane and the ERIC team are supportive of this effort, and we'll try to make sure they can be on both calls as well.

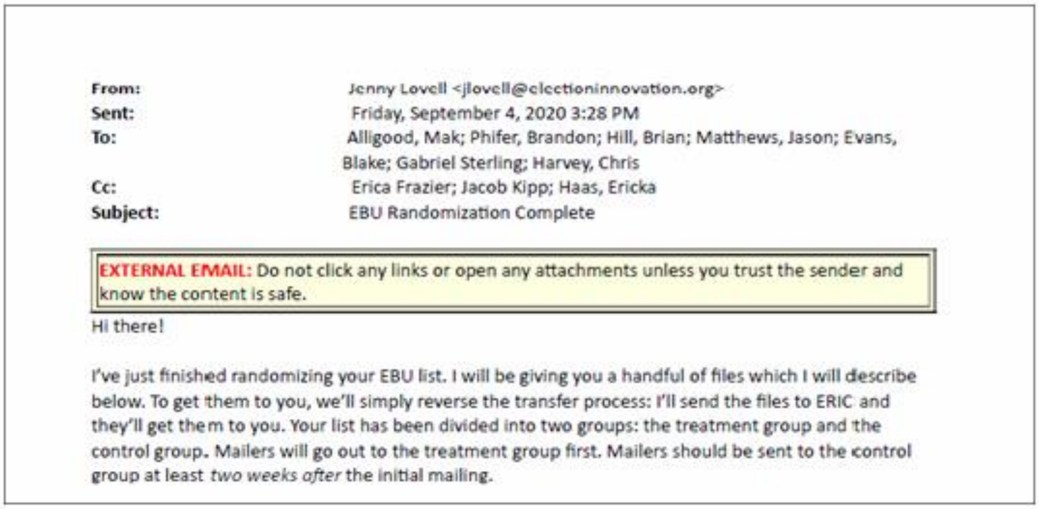
For now, we've created a doodle, and ask each of you (and any other potential attendees) to fill it out as soon as possible and let us know what times work. We'll then schedule the webinars, including video conference info, and you can pick which one works best.

Thanks! Have a great weekend!

David

David J. Becker | Executive Director and Founder
Center for Election Innovation & Research
1120 Connecticut Avenue NW, Suite 1040, Washington, DC 20036
(202) 550-3470 (mobile) | dbecker@electioninnovation.org
www.electioninnovation.org | @beckerdavidj

CEIR sends partisan mailers to voters or drivers warning them about *"election disinformation".* This technique was a partisan attempt to quell distrust in reported 2020 election results. Another Email shows that the top SOS election staff members were aware CEIR used the Georgia resident's data.



From: Jenny Lovell <jlovell@electioninnovation.org>
Sent: Friday, September 4, 2020 3:28 PM
To: Alligood, Mak; Phifer, Brandon; Hill, Brian; Matthews, Jason; Evans, Blake; Gabriel Sterling; Harvey, Chris
Cc: Erica Frazier; Jacob Kipp; Haas, Ericka
Subject: EBU Randomization Complete

EXTERNAL EMAIL: Do not click any links or open any attachments unless you trust the sender and know the content is safe.

Hi there!

I've just finished randomizing your EBU list. I will be giving you a handful of files which I will describe below. To get them to you, we'll simply reverse the transfer process: I'll send the files to ERIC and they'll get them to you. Your list has been divided into two groups: the treatment group and the control group. Mailers will go out to the treatment group first. Mailers should be sent to the control group at least *two weeks after* the initial mailing.

CEIR was supported by over $69 million in funding from Facebook founder Mark Zuckerberg through his Center for Technology and Civic Life (CTCL), yet another political adversary. Mr. Zuckerberg's blatant attempt to buy the outcome of the 2020 Georgia election is discussed previously is this study. [pg17]

g) ERIC is also a partisan organization founded by David Becker

The SOS first retained David Becker to host Georgia election security roundtables, despite a clearly defined track record as an extreme political adversary documented by Influence Watch. Becker's election work was widely known to be funded by George Soros through his Foundation to Promote Open Society while Becker was at Pew Charitable Trusts. Prior to joining Pew, Becker was an attorney at the highly partisan People for the American Way. Beginning in 1998 he served seven years as a trial lawyer in the DOJ where he was the lead opposing attorney in *Georgia v. Ashcroft* lower court hearings before Georgia won the case in the U.S. Supreme Court.

Influence Watch reports that Becker was the subject of a DOJ ethics complaint while employed at DOJ for offering the city of Boston help to defeat a DOJ lawsuit against them. They quote Brad Scholzman, then acting head of the Civil Rights division: "*It was the most unethical thing I've ever seen".* Hans Van Spakovsky, counsel for the Assistant Attorney General of the division, added that the investigation revealed his Emails contained *"…nasty, disparaging remarks about Republicans"* that were *"very unethical and unprofessional"*.

Becker has consistently maintained his rabid partisanship with many anti-Trump comments on the 2020 election such as: *"We have to understand that many voters are being subjected to a constant toxic diet of lies, fed to them by election losers and, in particular, the former president."*

h) ERIC has not been effective enough to comply with Georgia law

EAC statistics show non-ERIC states more effective at removing transferees annually than ERIC states by a margin of 2.1% for ERIC states to 2.9% for non-ERIC states. Nine states have left ERIC since 2020 including Florida, Alabama, Missouri, Ohio, Louisiana, Texas, West Virginia, Virginia and Iowa. Utah has also voted to leave. Less than half of U.S. states are members of ERIC. The remaining states have only about 80 million of the 210 million U.S. registrations or 38%. Further, only one Georgia border state is a member thus rendering ERIC ineffective for Georgia.

Mr. Mark Davis explained to the committee that several counties have more active and inactive registrations than 100% of the voting age population. The U.S. average is 78%. Few ineligible registrations had been removed until the last few years when citizens took it upon themselves to challenge those ineligible registrations that lingered on the voter registration database unnecessarily and unlawfully.

The General Assembly authorized the SOS to become a member of a nongovernmental entity "*to improve the accuracy and efficiency of voter registration systems".* ERIC has not improved accuracy or efficiency of our voter registration data as required by law. O.C.G.A. § 21-2-225

3. INELGIBLE VOTER REGISTRATIONS AND VOTES CAST

a) Georgia voter rolls contain roughly 20% problematic registrations

In a February 15, 2024 Senate Ethics Committee meeting, Dr. Rick Richards presented an analysis of Georgia voter roll accuracy to the Senate Ethics Committee. Despite Georgia being a member of ERIC, Dr. Richards found over 1.2 million problems with 7,711,670 million registrations. Examples of what Dr. Richards found include:

- 364,443 voters had moved out of county or their voting precinct
- 259,967 voters had moved out of Georgia
- 128,378 had non-deliverable addresses
- 220,899 had invalid addresses according to the United States Postal Service (USPS)
- 36,222 had addresses which were vacant
- 68,194 had addresses classified as unmailable by the USPS.

This shows clear examples of how ERIC has failed and how these invalid registrations are improperly left on the database exposing Georgia elections to fraudulent votes that can be cast for them.

in August 2023, the SOS decided to purge some of those invalid registrations. But as of October 2024, Dr. Richards found hundreds of thousands of problem registrations still on file when verifying addresses against the USPS Coding Accuracy Support System® (CASS). For example, the USPS CASS classified:

- 47,542 addresses as invalid
- 67,927 addresses were partial
- 12, 031 addresses were unrecognizable
- 21,250 addresses were businesses
- 8,053 addresses were P.O. Boxes

b) Thousands of fraudulent votes are being cast for ineligible registrations that remain on file

The failure to properly clean Georgia voter rolls has led to thousands of fraudulent votes being cast for the ineligible registrations that are left on the voter registration file. In some cases, these fraudulent votes are cast after the registration has been challenged as invalid. Here are three different types of problems from three different elections:

- A woman we will call Lacy, Voter Registration ID 08720588, was registered to vote from a nursing home in Roswell on June 27,2012. Two weeks later, on or about July 9, 2012, she passed away. She remained on the Fulton Co. voter registration list for over 10 years and was listed as Inactive on the October 20, 2023 voter roll. The voter history file shows an in-person absentee vote was cast for her registration during the November 7, 2023 General Election. Her My Voter Page as of November 10, 2023, showed her status as Active. It appears that she was moved from Inactive to Active without voter contact. [Complaint Pg 10]

- A former Fulton County registrant we will call Glen, Voter Registration ID 3566640, submitted a permanent change of address via the National Change of Address® (NCOA) system on June 1, 2001, and moved from Sandy Springs to Naples, Florida. He soon began voting in Florida and continued to vote there in the Novenber 5, 2024 election. However, he remained on the Fulton Co. voter registration file. His ineligible registration was challenged on August 7, 2024 pursuant to O.C.G.A. § 21-2-30 by Earl Ferguson. Fulton Co. denied the challenge claiming his inactive status was sufficient. Glen's credit for voting shows a vote was also cast for his ineligible registration on Election Day in Fulton's November 5, 2024 election. [Complaint]

- Voter Registration ID 10675883 and 1296054 are duplicates. They both represent a person we will call Anna who lives in the Virginia Highlands area. Votes were cast for both IDs in the Fulton Co. November 3, 2020 election. While one of these votes was obviously legitimate the other cannot be. If the system recorded two votes for one person the election could have never properly reconciled. [Complaint Pg 6]

These are just three of thousands of examples. A study of addresses for votes cast in the 2024 election as verified through the USPS CASS system by Dr. Rick Richards revealed:

- 20,665 votes cast from a business address;
- 11,921 votes cast from addresses not known;
- 7,972 votes cast from P.O. Box or Commercial Retail Mailing Agency;
- 47,229 votes cast from an invalid address.

A study of addresses for votes cast in the 2024 election analyzed according to the USPS NCOA system by Dr. Richards revealed:

- 135,403 votes cast where voter moved within or out of state;
- 4,046 votes cast where voter moved with no forwarding address;
- 363 votes cast where voter moved and registered within or out of state;
- 91 votes cast for registrations who moved and voted out of state.

The ineligible, invalid or problematic registrations that linger on the voter registration file appear to be traceable to a definitive number of causes. These include:

- The automatic opt-in of drivers who are not eligible to vote but are placed onto the voter registration database anyway;
- The inadequate validation checks performed when a voter is added to the voter registration database such as the failure to ensure the registrant has a CASS certified address;
- The refusal of counties to remove ineligible registrations when confronted with corroborating evidence the registrant has moved out of state, is deceased or otherwise ineligible to vote;
- The refusal of counties to investigate ineligible registrations when confronted with corroborating evidence that the registrant has moved out of state, is deceased or otherwise ineligible to vote.

The failure to properly clean Georgia voter rolls has led to thousands of fraudulent votes cast for ineligible registrations.

c) Some counties justify refusing to clean their voter rolls by misinterpreting NVRA

Georgia law O.C.G.A. 21-228(a) is clear that counties have a duty to periodically clean their voter rolls:

> *"(a) The board of registrars of each county or municipality shall have the right and shall be charged with the duty of examining from time to time the qualifications of each elector of the county or municipality whose name is entered upon the list of electors and shall not be limited or estopped by any action previously taken."*

HAVA also has a similar requirement in 52 USC 21083(a)(2)(A):

> *"(a) Computerized statewide voter registration list requirements*
> *(2) Computerized list maintenance*
> *(A) In general*
> *The appropriate State or local election official shall perform list maintenance with respect to the computerized list on a regular basis as follows:*
> *(i) If an individual is to be removed from the computerized list, such individual shall be removed in accordance with the provisions of the National Voter Registration Act of 1993"*

The corroborating NVRA requirement specified in 52 USC 20901(a)(4) states:

> *"**(a)**IN GENERAL*
> *In the administration of voter registration for elections for Federal office, each State shall—*
> ***(4)**conduct a general program that makes a reasonable effort to remove the names of ineligible voters from the official lists of eligible voters by reason of—*
> ***(A)** the death of the registrant; or*
> ***(B)** a change in the residence of the registrant, in accordance with subsections (b), (c), and (d);"*

However, certain counties refuse to comply with these federal and state laws even when presented with corroborating evidence that a given registration is ineligible or invalid. These counties frequently cite NVRA as an excuse claiming that the invalid registrations cannot be removed except by request of the registrant or after waiting two election cycles. However, the clear, plain text of the 52 USC 20901(a)(3) statute they quote shows that NVRA provides for invalid registrations to be removed *"as provided by State law":*

"(a)In General
(3)*provide that the name of a registrant may not be removed from the official list of eligible voters except—*

> ***(A)*** *at the request of the registrant;*
> ***(B)*** *as provided by State law, by reason of criminal conviction or mental incapacity; or*
> ***(C)*** *as provided under paragraph (4);"*

Georgia law OCGA 21-2-216 (f) explicitly requires the removal of registrations that are not qualified to vote:

> ***"(f)*** *No person shall remain an elector longer than such person shall retain the qualifications under which such person registered."*

OCGA 21-2-217(a) (1)-(15) specifies rules for determining residency including when residency is gained or lost. There is no requirement in Georgia law to maintain ineligible registration for two federal elections if the voter has not responded to notice from the county or state elections officials.

4. KNOWiNK POLL PAD SYSTEM SECURITY VULNERABILITIES

a) Counties are unable to produce a numbered list of voters for an election as specified by law

At least since 2020, county and state election officials have been completely unable to produce a numbered list of voters who voted after an election as prescribed in Georgia law. County election officials blame the inability to produce the list on KNOWiNK which is the data entry point for all in-person voting and the system of record for the list. [O.C.G.A. § 21-2-456(a)]

To circumvent this problem some election officials claim they cannot provide the list because it has time stamps that could compromise voter privacy. If true, they would be violating Georgia law. There is no direct link between a name on the list and a cast ballot. Voter check-in times and ballot casting times are not necessary in the same sequence. If election officials cannot prove who voted in an election, they cannot legitimately certify it, nor can they claim it is auditable. Without a list of voters who voted, any number of ballots could be cast for ineligible registrations.

In addition, county and state election officials have had difficulty producing an eligible list of voters in a timely manner prior to an election. Even in the few cases where the eligible voters lists were provided in a reasonably timely manner, they were not made public. Not being able to produce two of the most basic documents of elections, calls into question the security and integrity of those elections. [O.C.G.A § 21-2-401(b)]

b) KNOWiNK internet connectivity and synch issues jeopardize Georgia elections

Previous claims that poll pads are not connected to the internet have now been proven false. Georgia has traditionally employed secure online connectivity for early voting to update a voter record with credit for voting so that double voting can be prevented during the early voting period. This connectivity was delivered using ENet via a secure Virtual Private Network (VPN) between polling locations and the SOS office. With the purchase of KNOWiNK poll pads in 2019, that connectivity is now provided via a much less secure internet connection.

Despite continual emphasis on unnecessary risks, the SOS is also implementing additional risks of internet connectivity on KNOWiNK Election Day poll pads. This is being done under the pretext that it is needed for wait time monitoring even though waiting lines in Georgia have not been a problem and manual monitoring can easily be implemented and, in fact, it was used until the 2025 elections.

As a result, certain recently completed 2025 municipal and county elections experienced unnecessary internet connectivity issues on Election Day. Some precincts do not even have internet capabilities and were unprepared for such equipment.

Internet connectivity is unnecessary on Election Day since voters vote in only one precinct and can only check in once. Election Day poll pads traditionally have a resident copy of precinct voter data and have never needed internet connectivity. Exposing them to the internet runs the risk of allowing a bad actor to determine the number of voters who have voted in any given precinct so that the bad actor will know how many votes are needed for his or her chosen candidate to overcome the opponent and overturn the legitimate election results.

Yet another KNOWiNK security risk is being implemented by downloading the entire voter registration database to certain poll pads in an apparent effort to facilitate a long term “Vote Anywhere” initiative. Each poll pad only needs to have voter registration data for its precinct on Election Day or its county during early voting. These unnecessary downloads take hours and are especially problematic when new poll pads have to be set up in the event of malfunctions. Worse yet, it exposes the entire voter registration database to the risk of having a poll pad update voter data for a precinct in which it is unauthorized to do so.

Still another significant problem that county elections officials are experiencing is the inaccuracy of voter data across KNOWiNK, GARVIS and My Voter Page (MVP) platforms. County election officials complain that these systems are not in synch and provide different answers to the same question. That is because KNOWiNK is not integrated with the voter registration database. The poll pads require separate databases that are redundant with the main voter registration database. Contrast this cumbersome design to the ENet solution in which the voter registration database was updated directly through the secure VPN connection. Simply stated, the ENet solution was more secure, more efficient and less costly.

To again emphasize the critical nature of such remote exposures, consider that Dr. Stark, as head of the EAC TDGC resigned over the refusal of the EAC to adopt the TDGC recommendations to ban all remote connectivity for voting system components and he filed suit against them.

V. GEORGIA VOTING SYSTEM SECURITY SOLUTIONS

1. LEGISLATIVE IMPROVEMENTS (2021-2025)

a) Georgia made more legal election integrity improvements recently than any other state

Since the highly controversial 2020 election, the Georgia General Assembly has made many election security improvements through several election related bills. In fact, Georgia has been recognized by election integrity advocates as having made more election security improvements than any other state since 2020. Specifically, the General Assembly has:

- Banned outdoor drop boxes;
- Added visible watermarks and security paper features to ballots;
- Banned direct and indirect private money given to counties for elections;
- Made ballot images public records and physical ballots publicly available through ORRs;
- Replaced subjective envelope signature matching with more precise Drivers' License ID matching;
- Required posting of total ballots cast and left to count by vote type on Election Night;
- Required prior days' absentee ballots to be tabulated by 8pm on Election Night;
- Provided meaningful access for poll watchers to hear & see election processes;
- Improved chain of custody procedures for ballots;
- Added clarifications for valid voter roll entries and challenges;
- Provided independent funding for the State Election Board;
- Banned unverifiable QR Codes effective July 2026.

These changes represent solutions to a variety of election integrity problems and yet there is more work to be done to secure Georgia elections. However, the committee must distinguish between real and fake solutions.

2. FAKE VOTE COUNT VERIFICATION SOLUTIONS

a) Logic and Accuracy Testing cannot detect malware-based fraud

Since his 2002 letter to Georgia officials, VoterGA and this author have explained that **voting systems can be programmed to count differently during testing versus elections**. That means Logic & Accuracy (L&A) testing performed by all Georgia counties is inadequate to ensure vote count accuracy.

Most voting systems can count differently during testing by detecting the current date or by using ways to determine if they are running a test or election cycle. They can also be programmed to count differently after a certain number of ballots are processed, which is typically a very low number for testing. They can even be programmed to count differently after receiving a ballot with a certain abnormal combination of candidate selections. Voting systems can also be programmed to count differently after wirelessly receiving a signal. They can also be programmed to change the counts during an electronic upload of results.

For these reasons and more, Dr. Alex Halderman concluded in his Security Analysis that: ***"No practical method of pre-election or parallel testing can prevent malware-based fraud".*** His conclusion was confirmed to this committee by Dr. Stark and in court by Dr. Andrew Appell.

b) The RLA inventor has repeatedly explained why RLAs cannot be used to audit BMD systems

RLA inventor Dr. Phillip Stark wrote to GA election officials on February 18, 2019, and has testified in court that RLAs are meaningless for BMD elections because **BMDs are not auditable.** Some reasons for this are:

- A BMD cannot provide any original source of voter intent since it creates a machine marked ballot as the system of record of the votes;
- BMD ballots appear identical for any two voters who make the same selections and thus there is no way to ensure that the ballot was actually produced by a voter instead of a machine;
- A BMD makes the voter responsible for malfunctions and cybersecurity as Dr. Stark has already explained to the committee;
- An RLA cannot audit what a BMD showed to the voter, as acknowledged by state expert Juan Gilbert

Nevertheless, the SOS implemented an inappropriate RLA process and claimed that it verifies Georgia election results. The General Assembly subsequently codified it into Georgia law in HB316 and subsequent bills.

But a BMDs lack of auditability is not limited to RLAs. These same facts shown above are true for any type of audit on a BMD system, not just RLAs. There is no audit process that can effectively audit BMD systems for the reasons stated above. Therefore, BMDs should be eliminated in Georgia for lack of auditability.

c) Any audit of ballot images is illegitimate to claim a voting system is counting correctly

On Febuary. 19, 2024, the SOS announced that he was seeking funds to do a QR Code audit. Two days later, VoterGA explained in a Press Release that any "audit" of images is a "fake" audit. Nevertheless, the General Assembly approved that audit as part of SB189 while assigning it to the SEB with appropriate funding. The **SEB intended to conduct a legitimate paper ballot audit** but the SOS hijacked the process and the funds as Gabriel Sterling signed a contract with Enhanced Voting without the knowledge of anyone in the majority of the SEB. This was brought to the attention of the committee in its Clarksville meeting.

Enhanced Voting analyzed 2024 electronic ballot images, not paper ballots. Matthew Bernhard of Enhanced Voting acknowledged in the Covington meeting that **physical ballots should be audited, not images**. **Ballot images are never seen by the voter and cannot be a legitimate source of voter intent**. **The images may have been altered before the audit without detection.** This study explains how just such an alteration occurred with the Fulton County 2020 absentee ballot images. An audit firm would need extensive technical knowledge to detect such alterations and even so, could still not guarantee the originality of the votes.

Furthermore, the Enhanced Voting contract provided for counties to "fix" discrepancies found during the audit before the audit report was produced thus invalidating the legitimacy of the audit. Counties rescanned at least 92,000 ballots before the election, during it and after certification for reasons not documented in the audit report. This rescanning effort is documented in the 2024 Ballot Integrity Analysis produce by 30-year career image analyst, Phillip Davis, the leading expert on voted Georgia ballots.

For these reasons and more **the 2024 Enhanced Voting "audit" work was illegitimate and could not possibly determine that the "audit" confirmed originally reported election results**.

d) No type of audit is practical enough to ensure vote counts in close races are correct

This study has provided more than ample evidence that so called Georgia “audits” are horribly flawed and have been misrepresented to claim that they validate machine election results when they do not. Dr. Stark has confirmed exactly the same point in his testimony to the committee. Much false information has emanated from the SOS office about audits that many Georgia voters no longer trust any Georgia audit process. As Dr. Stark has explained to the committee, **auditing one race on a ballot does not prove any other race on the ballot was counted correctly nor does it prove the voting system counted the same type of race in another jurisdiction correctly.** Every contested race must be audited to ensure correct results.

While the RLA process appears to be the better and most practical way to audit elections, even this process breaks down in close races. That is why a full hand count was ordered to audit the 2020 Presidential race. Audits such as RLAs require more ballots to be audited as races get closer. Many extra ballots must be randomly selected to audit close races so that the risk limit can be reduced to a tolerable level. Even so, there is still a significant risk of the audit not detecting fraud or errors.

Georgia has typically employed auditing of enough ballots to conform to a 10% risk limit. More ballots for a race can be audited to reduce the risk limit further. But it is unrealistic to think that the risk limit can be reduced to under 5% without randomly selecting and auditing nearly all of the ballots in a very close race where the margin is less than 1%. **Simply stated, it would take far more time to randomly select the ballots needed to audit a close race than it would to simply hand count that race.**

e) Adjudication of scanned ballots is unnecessary and imposes a risk of vote manipulation

Adjudication of scanned ballots was introduced to Georgia by Dominion in the 2020 election. Prior to then, Georgia only altered ballots that were damaged and required duplication. Under the modified adjudication process, a selection bubble on a scanned ballot with under 10% fill is considered by the system not to be a vote, a bubble with over 20% is considered to be a vote and a bubble marked between 10% and 20% full is sent to adjudication **which allows third parties the opportunity to change or replace a voter’s ballot without the voter’s knowledge.**

American students of all ages have taken Scholastic Aptitude Tests (SAT), vocational knowledge quizzes and college entrance exams since they attended grade school. Students taking these types of tests do not rely on teachers to determine if they marked their answer sheet correctly. They are given proper instructions and assume that responsibility themselves. If they mark the answer sheet incorrectly, they are not given credit for their answer. No one adjudicates their answer sheets.

The premise that adult voters cannot fill out their ballot correctly and must have other individuals determine who they really wanted to vote for is a recipe for election fraud. Not only could a partisan adjudication team change voters’ ballots, but **storing ballot images in an “electronic bucket” awaiting adjudication is an invitation to bad actors for electronic vote manipulation**. Adjudication delays the results tabulation process and makes all ballots vulnerable to electronic vote manipulation. The adjudication process can be eliminated simply by changing the scanner settings to eliminate the adjudication range.

3. REAL BALLOT SECURITY SOLUTIONS

a) Unique ballot identifiers will help prevent duplication and injection of fraudulent ballots

While the General Assembly has made strides in providing ballot security features like watermarks through SB202 (2021) and HB974 (2024), unique identifiers for ballots are still needed to detect duplication and help prevent fraudulently injected ballots. **Ballot Identifiers uniquely identify the ballot, not a voter, as some have falsely claimed.** Unique identifiers can be applied to pre-printed forms or by Ballot on Demand printers. Uniquely identified ballots can be manually or electronically randomized if needed to maintain voter privacy when distributed.

b) Absentee ballot delivery must be ensured by address verification and delivery tracking

Although this study has focused mostly on electronic aspects of voting system security, absentee voting security must be addressed to provide a comprehensive security solution. County election offices do not currently track whether or not ballots that are mailed to voters are actually received by the intended recipient. In addition to its cloud-based security flaws, **the current voter registration system does not have adequate means to ensure accurate residential addresses are being entered into the system and that the addresses are deliverable via mail.** Tracking and confirmed delivery from postal and third-party services are now sophisticated enough to be implemented to ensure that ballots are actually delivered to the intended voters. The USPS CASS system can now be utilized by counties to ensure accuracy of voter roll addresses. The USPS Delivery Point Verification (DPV) system can also be employed to ensure that each mailing address is deliverable. USPS or third-party tracking can then be employed to ensure that voters actually receive the absentee ballots they requested.

c) Absentee ballot legitimacy must be ensured by requiring IDs for each ballot deliverer

Voters who vote in person early or on Election Day must provide an ID to prove they are qualified to vote. While an ID may be required to obtain an absentee ballot by mail, **no ID is required to return a mail-in ballot. This is an open door for mail-in ballot fraud and potential Equal Protection violations against in-person voters.**

Although the General Assembly thankfully banned unsecure outdoor drop boxes, Georgia law still allows for ballots to be returned using drop boxes set up in election offices and some early voting poll locations. No ID is required to use a drop box or to return a ballot in person at an election office.

ID verification is needed when casting all absentee ballots to ensure the legitimacy of those ballots and fulfill voter equal protection rights under the U.S. and Georgia Constitutions. That requires absentee ballots to be delivered in person to an election office or polling location so that ID verification of the voter or designated deliverer can be performed.

d) Absentee ballot designated deliverers can be used to replace fraud-prone mail-in voting

Mail-in voting has been a source of election fraud for years. It can be eliminated by allowing each recipient of a mailed absentee ballot to use a designated deliverer to return their ballot for them if they are unable to return it themselves or unable to vote on Election Day. A recipient could specify up to three possible designated deliverers authorized to return their ballot to help ensure that at least one would be available when needed for the return. The deliverer would provide their ID when returning the ballot to an election office or poll location for a qualified voter who cannot deliver their ballot in person.

e) Hand Marked Paper Ballots will provide an auditable record of voter intent

Student tests are conducted using hand marked paper answer sheets. The students mark a bubble that identifies their answer to each question asked during any given test in the same manner that voters mark an absentee ballot. **When casting a ballot, there is no reason why in-person voters cannot apply the same ultra familiar hand marked paper technique they used throughout school to take most of the classroom tests that were administered to them.**

Hand marked paper ballots establish auditability that a BMD touchscreen cannot possibly offer. They provide uniqueness of markings that can help detect when duplicates are accidentally or intentionally counted. They also offer a permanent, undisputed record of voter intent for each ballot cast, provided that they are not adjudicated. Simply put from an auditing perspective, **nothing should come between a voter and their ballot.**

A hand marked paper ballot implementation would also be consistent with the Georgia Supreme Court ruling that O.C.G.A § 21-2-437 applies to our BMD system. It states: *"Any ballot marked by anything but pen or pencil shall be void and not counted…"* **There is no cost justification for filling out ballots with what are essentially $3000 electronic pencils.**

f) Ballot on Demand printing addresses pre-printed form concerns for early voting locations

The only true objection to hand marked paper ballots comes from county election officials who are concerned over maintaining many different ballot styles during early voting where voters from many different precincts can vote at one location. This can be mitigated through Ballot on Demand (BOD) printing at early voting centers.

BOD printing can be integrated with the poll pad check in process and used to print the correct ballot style for a voter when the voter checks in at a polling location. BOD printers can also provide a unique identifier (ID) for a ballot based on the Printer ID and sequence number of the ballots printed. The unique IDs provide an additional layer of security to help prevent and detect unauthorized ballot duplication.

g) Ballots must be received by election day to prevent fraud and comply with federal law

In-person absentee voting is required to be completed on the Friday before Election Day but UOCAVA mail-in votes are accepted up to three days after Election Day. **Federal law has no such provision for accepting ballots after Election Day.** Late phantom absentee votes diluted the legitimate votes cast in the 2020 General Election by in person Georgia voters who complied with federal and state law.

The vulnerability of having post-Election Day votes change the outcome of the election results, as happened in 2020, can be eliminated just by mandating that all absentee ballots must be received by the close of business on the day before Election Day. UOCAVA voters are not truly harmed since they are normally mailed ballots three days before remaining absentee ballots are first mailed to voters. This safer and more practical deadline allows the counties to distribute all of their absentee ballots to the precinct for counting on Election Night.

h) Free public access to an independent copy of ballots will restore voter confidence

In addition, the General Assembly must legislate "no excuse" election transparency of all ballots and records to ensure the voters have transparency in elections and protect voters from counties who do not want to comply with recently implemented Georgia transparency laws in SB189**. These SB189 laws must be enhanced to ensure they apply to all ballot custodians. The enhancements must also remove the excessive financial burden on Open Records Requestors by making ballots available to the public for free.**

4. REAL VOTER REGISTRATION SECURITY SOLUTIONS

a) Georgia's voting registration data must be in-house for control and security

Georgia voter data must be accurate and trustworthy. Georgia counties and their voters cannot be held hostage by a poorly designed, poorly implemented GARVIS system that has thousands of errors and lacks adequate control and protection of voter data. **To achieve accuracy and provide adequate security, the Georgia voter registration system must first be removed from the hands of third parties and non-U.S. citizens and returned in house where it can be properly secured.**

The source and responsibility for Georgia voter data are the counties. Therefore, **the counties should have exclusive control of their voter data and their voter registration system**. Then, they can produce reports such as numbered voting lists that they are not currently able to provide. It is time for a fresh approach.

The federal government is making available the tools necessary for counties to properly maintain their voter lists. This includes:

- The DHS Systematic Alien Verification for Entitlements (SAVE) system to verify citizenship;
- The Social Security Administration (SSA) SSN Service and Death Master File to help confirm voter eligibility;
- The USPS CASS, DPV and NCOA systems for accurate residential address entry, delivery verification and change of address notifications;
- Department of Justice (DOJ) National Crime Information Center (NCIC) to identify felons who are not qualified to vote under Georgia law.

Traditional voter registration systems contain voter registrations that are hopelessly out of date and can never be made current. Counties can be better served simply by creating a dynamic voter qualification list for each election. The election eligibility list would be initiated from the list of numbered voters in the previous election and supplemented by new registrants. Accuracy can be improved by processing address change notices from the DDS state driver license system. This eliminates the need to carry over obsolete, ineligible registrations for a decade or more and reduces the risk of having those ineligible registrations used to cast fraudulent votes. Details about dynamic voter qualification are in VoterGA's SAFESTEP election procedures described later.

b) Georgia can clean its voter rolls without giving Georgia voter and driver PII to ERIC

The SOS has given PII of both Georgia voters and drivers to ERIC without their consent. The committee determined that **ERIC has imposed unwarranted restrictions on Georgia** and can continue to do so in the future. All of this is done under the guise of keeping Georgia voter rolls clean.

Driver PII is obviously not needed to clean voter rolls. Voter PII does not have to be given to a third party to clean voter rolls. Any state can take the initiative to clean its voter rolls without a third-party product. At least 40 states already exchange data directly with each other through the American Association of Moter Vehicle Administrators (AAMVA).

If an ERIC replacement is deemed needed, several tools are available that are far more effective at cleaning voter rolls than ERIC. **These tools access many additional sources of data, contain many more vote records for comparison and do not require PII to make those comparisons**. Two such examples are ELLY – The Elector List^{TM}, which is built for counties and the general public, as well as Psephos^{TM}, its sister product, which is built for states.

For comparison purposes ERIC is used in about 22 states, employing about 82 million voter records for comparisons. By contrast, ELLY – The Elector List^{TM} and Psephos^{TM} utilize over 200 million voter records from 46 states, 2 ½ times or 120 million more records than ERIC. They impose no constraints on counties or states like ERIC does for using the product.

ERIC relies primarily on NCOA data and the SSN Death Master File which has no full date of birth and is not updated in a timely manner. ELLY – The Elector List^{TM} and Psephos^{TM} provide far more accurate comparisons by accessing additional data sources shown by asterisks below:

- Voter list data from each state Secretary of State
- Voter history data from each state Secretary of State
- Corporate data from each state Secretary of State
- Felon data from the state
- National Change of Address data
- Social Security Number Death Master File
- Property zoning codes, property class codes, land use codes from all US Counties*
- Property tax data, homestead exemption and sale dates & amounts from all US Counties*
- Property description with number of rooms, bedrooms, and owner occupancy from all US Counties*
- Residential Address format corrections from the USPS Coding Accuracy Support System*
- Residential Address information corrections from the USPS Coding Accuracy Support System*
- Mailing Address format corrections from the USPS Coding Accuracy Support System*
- Mailing Address information corrections from the USPS Coding Accuracy Support System*
- Non-Residential Address data from the USPS Coding Accuracy Support System*
- Non-Deliverable as addressed data from the USPS Coding Accuracy Support System*
- Obituary data from funeral homes, newspapers*
- Proprietary Change of Address (PCOA) data, multi-source collaborated (e.g., credit card company)*
- Corporate data from Google® Business*
- Maps, street and sky view images from Google®*

What's more ELLY - The Elector List^{TM}, made its incredibly simple, yet sophisticated user interface available to the public, making it fully transparent for voters. In that way, it can serve as an assistant by performing the first steps of identifying problem registrations for county election officials to confirm.

This illustrates that more effective and efficient voter roll management solutions are available without compromising voter PII and especially PII of Georgia drivers that can be unrelated to voter registrations.

c) Replace unnecessary poll pad internet connectivity with secure private networking

As previously explained, Georgia's poll pad implementation recently became riddled by problems, risks and vulnerabilities involving unnecessary internet connectivity, unnecessary voter data redundancy and resulting voter data synchronization issues that led to inaccurate voter data reporting to county officials.

Establishing a dynamic voter qualification system under county control for each election allows the county to reduce their dependence on a poll pad system or outsourced SOS data to maintain eligible voters and produce a numbered voters list for each election. Until such time, **unnecessary remote connectivity must be eliminated from the poll book system to make it more secure. Election Day poll pads do not need remote connectivity**. There is simply too much risk of a bad actor being able to use real time poll data to determine how many votes are needed to change the outcome of an election through existing voting system remote connectivity. Therefore, recent changes in poll books must be rescinded so that the software can be secured for the 2026 election**. Any future poll pad connectivity should be deployed through a secure Virtual Private Network (VPN)** in the same manner that the ENet solution provided. Integration with the voter registration database must also be achieved to eliminate redundancy and synchronization errors that have led to inaccurate voter data reporting.

5. REAL VOTE COUNT SECURITY SOLUTIONS

a) Publicly recorded hand counts

As previously explained, there is no testing procedure that can prevent malware-based fraud and no audit procedure that is practical enough to ensure vote count accuracy in close races. **The only vote count verification method that can truly restore voter confidence in Georgia election outcomes is a full, publicly recorded hand count of contested races for each Georgia election**. Publicly recorded hand counts eliminate:

- Cybersecurity threats;
- Expensive scanners, tabulators and servers;
- High priced election support consultants;
- Costly hardware maintenance;
- Pricey software agreements;
- Equipment storage facilities;
- Complex training requirements;
- Inadequate Logic & Accuracy testing;
- Insufficient audit procedures;
- Unverifiable QR codes;

- Secret vote counts;
- Secret proprietary software;
- Time consuming, out of date and compromised EAC certifications;
- Third party security issues;
- Forensic examinations;
- Reliance on unknown software processes.

The costs and time savings for the above far offset the costs incurred to hire polling location counters which can be a mostly volunteer and student counting staff.

b) An SB303 solution provides hand marked paper ballots and publicly recorded hand counts

As previously explained, the paper ballot statutes recognized by the Georgia Supreme Court as applicable to Georgia's elections outline extensive hand counting provisions that are already codified. SB303, a currently active bill, conforms to these provisions. O.C.G.A. § 21-2-437.

SB303 provides for publicly recorded hand counts at the precinct where votes were cast as well as hand marked, paper ballots. The bill is sponsored by Senators Colton Moore, Steve Gooch and Greg Dolezal. It can be rather easily amended in the upcoming session to achieve the solutions specified in this study.

c) Hand count testing of actual Georgia ballots has shown it can be accurate and timely

This study has shown several real-life examples illustrating that hand counting is more accurate than current Georgia machine counts. It has provided evidence that there is no mechanism under which machine counts can be trusted to be accurate.

A recent hand count demonstration test with copies of actual Georgia ballots shows that **hand counting can be conducted at the precinct in a timely manner**. Based on the demonstration results, it is safe to conclude that 9 federal, statewide, and General Assembly races can be counted with 100% accuracy in an average precinct of 820 ballots with a 16-person team in 2 hours and 45 minutes.

The time it takes to count the ballots can be adjusted based on the number of ballots, races to count and team members who will do the counting. The keys to success are:

- Keeping the current precinct sizes at 1500 to 2000 registered voters as most are now;
- Employing fresh teams of people to conduct the hand counts when the polls close;
- Using supervised volunteers and college or high school students to keep costs minimal.

A recent hand counting implementation in Milton 2023 municipal election found so many enthusiastic respondents that officials had access to far more volunteers than they needed for counting team positions.

VI. PRIORITIZED SOLUTION SUMMARY

1. TEN MOST URGENT SECURITY SOLUTIONS

The following list represents solutions to what VoterGA believes to be the top ten election security issues facing Georgia. **Most of the solutions can be implemented with minimal procedural adjustments, nominal costs and simple legislative code changes**. Only two or three of the proposed solutions require expenditures of state funds.

a) Georgia's voting system must be removed from service to secure the 2026 elections

This study provides overwhelming unrefuted court expert witness testimony and evidence that Georgia's voting system is uncertifiable, unsecure, configured for remote access and was accessed remotely by foreigners during Georgia elections. Perhaps even worse is the forensic evidence that shows county election program files were modified without detection after being installed, election results have been altered through tampering and an uncertified program compiler was installed which allows a bad actor to develop malware and distribute it to other county election components without detection for any election.

The simple solution to this unacceptable voting system security dilemma is to unplug this system and employ hand marked paper ballots with publicly recorded hand counts. Public recorded hand counts deter the possibility of cheating, eases current public divisiveness generated by never knowing for sure who really won an election and provides massive cost and work effort savings as explained in a previous section.

SB303 currently provides the road map for both hand marked paper ballots and publicly recorded hand counts. BOD printing can overcome any remaining objections to hand marked paper ballots by eliminating the need for pre-printed ballots in early voting locations. **Unique ballot identifiers for all ballots will help prevent duplication of any type of ballots and deter fraudulent injections of fake ballots into election results.** Potential legislative changes for these enhancements are shown in the Appendix.

b) Georgia must implement internal ballot fraud prevention measures

Although the legislature has taken many steps in the past few years to improve security and prevent fraud there are still a variety of loopholes that must be closed. Therefore, **measures must be adopted to prevent duplication of ballots, to ensure that ballots accepted are being cast by legitimate voters and to prevent counterfeit ballots from being injected into actual election results.** Specific solutions outlined in previous subsections of this study include:

- Create unique identifiers on ballots to prevent unauthorized duplication;
- Use the USPS CASS system to ensure voter addresses are accurate ;
- Use the USPS DPV system to ensure voter addresses are deliverable;
- Verify IDs of each ballot deliverer to ensure ballot legitimacy.

Proposed legislative changes for these provisions are shown in the Appendix.

c) Georgia must codify ”no-excuse” free, public access to ballots

The General Assembly has made a variety of election transparency improvements in recent legislative sessions. **Nevertheless, the committee heard how Fulton County has stalled for years in producing 2020**

election ballots for civil cases, criminal court, the SEB and now even the criminal and civil division of the DOJ. The committee also heard how other counties such as Forsyth want up to $49,000 just to produce a copy of ballots for an election cycle.

Digital copies of ballots, electronic files and other election records must be produceable under custody and control of election officials, with public observation of such copying, and made publicly available immediately upon certification of each election. A single electronic copy can then be given to any requestor for low-cost record production. A standard 600 dpi, 16-bit color copy of ballots produced independently of the voting system and made publicly available on demand would help ensure accuracy of election results and restore public trust in elections.

The legislature took steps to make just such an independent 600 DPI electronic copy of ballots publicly available with SB189 in 2024. Some counties have since begun producing independent, high-resolution scans of the actual ballots for each election and will provide the electronic copy free to any requestor.

But many counties are now making excuses, such as finger pointing between the Boards of Elections and the Clerk's office over custody or charging exorbitant fees mentioned in this study to avoid complying with the law. **The legislature must enhance SB189 transparency provisions to prevent the subversion of Georgia election transparency law.** Simple legislative changes to tweak the SB189 transparency provisions are shown in the Appendix.

d) Georgia must establish an unbiased, efficient state election court to hear cases

Georgians whose votes were diluted in the 2020 election by counterfeit ballots and other means have suffered the greatest voting rights violation in Georgia history. They have endured five years of stalling tactics initiated by election officials to prevent ballots from being made publicly available. Public transparency is needed to verify election results and determine the remedies required to prevent a reoccurrence of 2020 ballot box stuffing that obviously occurred. **Superior Court judges have been accomplices in allowing potential criminal election activity to go unchecked.** They have dismissed cases on false standing rulings and delayed justice for years to achieve partisan objectives.

The root of election judicial problems is that all election cases must originate in Fulton County, the epicenter of Georgia election problems. If we have learned anything in this debacle it is that Fulton County judges are simply not willing to rule against Fulton County. Worse yet, they may even take unethical steps to ensure they don't have to rule against Fulton County.

Election related lawsuits must be removed to a state election court that can be set up in a manner to be more unbiased and efficient in processing cases. The court could be staffed with retired judges and mostly part-time personnel that will keep costs low. Care must be taken to ensure it has full authority to resolve cases brought before it.

The court would provide jurisdiction for elections claims under Title 21 within the business court. It could convene as a 3-judge panel with direct appeal to the Georgia Supreme Court. Each circuit could name two retired judges who would be chosen at random to preside. Of course, no judge from a circuit at issue in the contest would be eligible. Potential concepts that can be incorporated into legislative changes to establish such an election court are shown in the Appendix.

e) The SEB must be fully independent to ensure honest election security investigations

This study has provided overwhelming evidence that election security investigations are continually compromised by SOS investigators since they were given power to investigate elections in 2007. The study explained the politicization of 2008 election investigations, including one that overturned election results. It documents the cover-up of the 2017 breach at KSU CES and the investigation of 50,000+ unsourced certified votes in the Fulton County 2020 election for which investigators told the SEB that there was nothing to see.

These examples illustrate the need to **make the SEB fully funded, fully independent and in charge of election investigations.** Its five-member appointment structure makes it the most unbiased entity to perform election investigations and the most knowledgeable to perform preliminary investigative activities prior to criminal prosecutions. Proposed legislative changes that restore some of the independence of the SEB that it had in 2006 and earlier are shown in the Appendix.

This study has also pointed out the role of the SEB chairman in continually attempting to prevent the Fulton County 2020 election from being properly investigated through SEB2023-025. This case is the most significant complaint of election violations in SEB history. The chairman's actions cited are only the tip of the iceberg of subversive activities he undertook in repeated attempts to prevent a legitimate Fulton County election investigation resulting from SEB2023-025. **The legislature must use its authority to appoint a new chairman who can work with the SEB to ensure the integrity and security of the 2026 elections.**

f) Georgia voter data must be moved back in house to resolve security issues

This study has provided evidence that Georgia's voter registration data was outsourced to a Salesforce cloud without legislative authority to do so. The outsourcing was performed in large part, by inexperienced individuals who are not U.S. citizens. **The result was a system that was delayed a year, incurred over 3500 support tickets when implemented, provides data that county officials can't trust and is still unsecure**.

The cloud uses layers of third-party software vendors proven to have political agendas not favorable to Georgia. **At any time, they could decide to refuse service and even refuse Georgia access to our own voter data.** Some already have such a proven adversarial track record. **This is an unacceptable risk that should have never been allowed to occur in the first place.**

The legislature must take the appropriate steps to legally ensure that all voter registration data is brought back in house. At the same time, **it should consider replacing this unsecure, constantly out-of-date system with a new county system that qualifies eligible voters dynamically for each election**.

This study has pointed out the unnecessary internet security risks imposed on the voter registration data as well as the redundancy and synchronization problems of having multiple voter registration sources. The legislature must move to eliminate these risks by ensuring that secure in-house VPN or similar connections are used for any communications in lieu of internet connectivity and that a single system of record of voter data is implemented at the county level where the data truly originates and is maintained.

Potential legislative changes to clearly prohibit third party vendor involvement in maintaining, transmitting or controlling Georgia voter roll data are shown in the Appendix.

g) Sharing of Georgia voter and driver PII must be eliminated to protect privacy

The committee heard that **Georgia is currently transferring both voter and driver PII to ERIC**, a third party, **based on an agreement signed without the consent of Georgia voters or drivers.** The committee also heard that ERIC, which is partisan in nature, stores Georgia's data in a location unknown to Georgia voters or drivers and has transferred the data to another third party, CEIR, that is partisan in nature. **Our Georgia voter data has been used for partisan get out the vote efforts and partisan disinformation or misinformation campaigns all without our consent.**

ERIC imposes these and other constraints upon the state of Georgia under the guise that it needs our PII to help clean up Georgia voter rolls by comparing the data with other states. However, **ERIC is not even used by half the states in America,** is employed by only one bordering state to Georgia and has lost 9 member states since the 2020 election.

Dr. Rick Richards has explained to the legislature that **PII is not needed to maintain clean Georgia voter rolls** and no imposition should be imposed on a state by any third-party software vendor to do this. His product, ELLY – The Elector List^{TM}, utilizes over 200 million voter records from 46 states. That is twice the number of states and 2 ½ times or 120 million more records than ERIC. It does not use PII and it imposes no restrictions on counties or states as ERIC does to Georgia.

Georgia is fully capable of cleaning its voter rolls without third party impositions, privacy violations and secret transfers of Georgians' PII to third parties. The legislature must discontinue the unnecessary transfer of PII data to ERIC and other third parties and take steps to ensure their new requirements are enforced. This can be accomplished with the current version of HB215, sponsored by Rep. Momtahan and Chairman Fleming who both serve on the committee.

h) Georgia must have comprehensive legislative reforms to achieve voter roll accuracy

Once the platforms for Georgia's voter registration database are secured, voter roll data must be scrubbed. This study has provided detailed evidence that Georgia voter roll records are grossly inaccurate for a variety of reasons. **Comprehensive legislative reforms are needed to force the SOS and county offices to periodically clean and maintain the voter rolls and help to ensure that bad data is not entered into the system when new registrations are added**. For example, Georgia code changes are needed to:

- Ensure that only those drivers who proactively Opt-in to vote are added to the voter rolls;
- Provide USPS CASS verification of addresses when a new registration is entered;
- Require DDS address changes to be accurately applied to the voter rolls database;
- Impose penalties on counties that do not properly maintain their voter rolls;
- Require counties and the SOS to publicly post the Numbered List of Voters for each election;
- Require counties and the SOS to publicly post Eligible Electors List for each election.

Proposed legislative changes to accomplish these objectives are included in the Appendix.

i) Georgia must replace fraud-prone mail-in voting with designated ballot deliverers

This author was present when counterfeit mail-in ballots were found by senior poll managers and confirmed by audit monitors during the Fulton County hand count audit conducted on November 14-15, 2020. The senior poll managers were told to continue counting them anyway. Mr. Evans later acknowledged during a courtroom cross examination that **Georgia has no policy to mitigate illegitimate ballots.** Instead of immediately getting to the bottom of this election breach, **state and local officials entered into a five-year cover-up that has kept the counterfeit ballots concealed in secrecy to the point that they are still being subpoenaed or requested by three civil cases, a criminal case, the SEB, the DOJ civil division and the DOJ criminal division.**

This highly vulnerable mail-in method of voting was exploited during the 2020 election to the extent that it appears it was used to overturn Georgia's legitimate 2020 General Election results after the election was conducted. For example, test ballots were created prior to the election and left unsecured. These may have been the ballots that were injected into the system as mail-in ballots.

Ironically, a simple solution to this problem that would also preserve convenience for Georgia voters is to require that voters to designate a deliverer for their absentee ballots rather than placing them into a fraud-prone mail system that can be subverted and even used to submit fraudulent ballots that were never mailed. As previously explained, an absentee voter could specify up to three designated deliverers on their application. The deliverer's ID would be checked when the ballot is delivered in person at an election office or early voting poll location. Some of the code changes needed to replace mail in voting with designated deliverers are suggested in the Appendix.

j) Ballots must be received by Election Day for compliance and fraud prevention

This study has provided ample evidence from Secretary Raffensperger's own words and reports that over 200,000 phantom ballots from unknown sources were injected into the 2020 election results after Election Day. The ballots clearly overturned the real election results after 158 of 159 counties completed reporting.

The General Assembly cannot allow election results to be overturned after Election Day again. As previously explained, these late phantom votes diluted the legitimate votes cast by voters who complied with federal and state law. **Federal law has no provision for accepting ballots after Election Day.**

The legislature must move to mandate that all absentee ballots be received on the day prior to Election Day. This includes UOCAVA ballots, which already get a three-day head start in ballot distribution. Alternatively, a voter or their designee could deliver the ballot with identification at the precinct on Election Day however, a designated deliver would be required to submit the ballot provisionally since the precincts would have no access to the absentee ballot application to verify the Deliverer ID.

These reasonable and practical deadlines allow counties time to distribute all of their absentee ballots to their precincts for counting on Election Night. Proposed legislative changes to achieve these deadlines are shown in the Appendix while the counting procedures can be supplied upon request.

2. FEDERAL SECURITY COMPLIANCE CONSIDERATIONS

Although this study has focused on what Georgia can do to improve election security, it would be remiss not to consider potential federal implications that could require additional aspects to Georgia election enhancements for federal elections. The designation of election systems as **critical infrastructure** and the **growing election security crisis** may dictate federal action by the end of this year. The President has issued EO 14248 and stated more **election security orders are imminent**. In addition, drafting of the ***Make Elections Secure Again* bill** has long been underway.

With that in mind, VoterGA developed full election life cycle procedures to achieve objectives stated by the President and members of Congress. The procedures, entitled *Securing Accurate Federal Elections with Safe Transparent Election Procedures*, or SAFESTEP, are included here. They provide a complete "how to" road map of high-level election activities to fulfill the January 6, 2017, DHS designation of elections as critical infrastructure and comply with any expected EOs based on the President's stated election security initiative.

The life cycle activities in SAFESTEP are comprised of end-to-end security provisions from the time ballot paper is created until any election challenge is adjudicated. Provisions intended to end the national election security crisis, some of which have already been incorporated by Georgia, include:

1. Serialized, watermarked ballots with security features to prevent duplication;
2. Photo voter identification to authenticate all voters;
3. Proof of citizenship to ensure eligibility of all voters;
4. Replacement of all mail-in balloting with a designated deliverer to prevent fraud;
5. Limited absentee voting for specific excuses to mitigate absentee irregularities;
6. Directly hand marked paper ballots to provide auditability of all ballots cast;
7. Publicly recorded hand counts of the votes at the precincts where cast to ensure accuracy;
8. Dynamic, verified voter qualification established for each U.S. election to avoid reliance on inaccurate, outdated voter rolls that span multiple election cycles;
9. Address delivery verification, tracking and confirmed delivery to ensure the correct recipient receives each sent ballot;
10. Assurance that all ballots are accepted by Election Day to comply with federal law;
11. Comprehensive chain of custody to secure all ballots and records employed during the election;
12. Public availability of all ballots, files and processes used in each election to ensure transparency;
13. Prevention of foreign influence, private funds and other interference in United States elections.

The activities defined in this life cycle extend the VoterGA security recommendations for Georgia. The committee is encouraged to consider these additional provisions as needed.

VII. ABOUT THE AUTHOR

Garland Favorito, co-founder of VoterGA, is a career Information Technology professional with over 40 years of experience in computer programming, business systems analysis, data administration, internet systems design and systems architecture as well as systems development methodology.

As a systems development methodologist, he developed, enhanced and consulted in full life cycle methodologies needed by large scale corporations to implement mission critical application systems. These methodologies include systems analysis, database design, re-engineering, application development, structured testing, auditing measures, quality assurance and many other time-tested procedures. The methodology products he developed or enhanced were marketed to large corporations and top national accounting firms who provided the methodologies with their branding to their customers during consulting engagements.

Mr Favorito also consulted nationally in all aspects of large-scale systems development. His industry experience includes banking, financial systems, health care, accounting, manufacturing, inventory, purchasing, retailing, utilities, telecommunications, insurance, government, software development and the residential service industry.

For the last 13 years of his professional career, he served as an internet systems analyst developing and enhancing online banking applications for corporate, retail and small business transaction systems at a leading financial institution. He helped design, develop and integrate their Online Identity Management component which protected the identities, accounts and financial transactions of over 1.5 million customers from cyber intrusion. His cyber protection experience includes multi-factor authentication, silent mode data collection, software token messaging, out of band authentication, challenge response subsystems, encryption key authorization and software firewall architecture.

Mr. Favorito also has 25 years in voluntary part-time and full-time election integrity advocacy and voting system technology experience. He has served as an audit monitor, recount monitor, tabulation observer, mail-in ballot processing observer, poll watcher and audit monitor coordinator in the 2020 election. He has made hundreds of educational presentations throughout the state. He has published & presented research papers for national conventions and recommendations for state system evaluations.

Mr. Favorito has successfully advocated for passage of many legislative improvements and authored rules adopted by the State Election Board. He has testified before committees and sub committees in the Georgia General Assembly and State Election Board. He also serves as an expert witness on election integrity, voting system technology and Georgia election security issues both nationally and in Georgia.

VIII. ABOUT VOTERGA

Voters Organized for Trusted Election Results in Georgia, VoterGA, was established in 2006 as a nonpartisan, non-profit, all-volunteer, dues free organization. It has led the election integrity movement in Georgia for roughly 20 years and has over 20,000 supporters and followers. It is dedicated to restoring the security and integrity of Georgia elections through verifiable, auditable and recount-capable voting.

VoterGA educates voters, legislators, poll workers, poll watchers, and civic groups throughout the country on a variety of election related topics while providing free expert witness testimony in high profile national cases.

The organization has filed a variety of litigation to defend voting rights of Georgians and has successfully advocated for many legislative changes and several State Election Board rules to improve election integrity.

VoterGA founders have been plaintiffs in landmark U.S. District Court and Georgia Supreme Court cases. A U.S. District Court case found Georgia's previous Direct Recording Electronic (DRE) voting system to be constitutionally deficient. A landmark Georgia Supreme Court case confirmed that Georgia voters have always had standing to sue government agencies and officials who violate the law.

VoterGA currently has four active court cases regarding irregularities and potential fraud in both 2020 and 2022 Georgia elections including the potentially illegal outsourcing of Georgia voter data to a cloud. We are committed to continuing and winning our fight to protect Georgia voters and secure Georgia elections.

IX. APPENDIX OF POTENTIAL LEGISLATIVE CODE CHANGES

This appendix contains potential legislative changes that can improve Georgia's voting system security. They are offered as guidelines only and must be fully vetted by Legislative Counsel.

1. VOTE COUNT SECURITY

a) Provide free, public access to an electronic copy of voted election ballots

Said chapter is amended in Code Section 21-2-493, relating to the production of ballots for an election as follows:

(j.2)
(1) On or after January 1, 2025, in the event that a superintendent or a Clerk of the Court or any official who maintains custody of the ballots (Custodian) receives a request pursuant to Code Section 50-18-71 for scanned ballot images at a resolution higher than the ballot images available from the Secretary of State pursuant to subsection (j.1) of this Code section, and such request is received following the final certification of the results of the election in which such ballots were created, the superintendent or Custodian shall, consistent with Code Section 50-18-71, produce digital scans of the requested ballots at a resolution of no less than 600 dots per inch and deliver such scans at no cost to the requestor. A person making a request pursuant to this subsection may observe the scanning and related handling process, but under no circumstances shall anyone other than an authorized election official touch or handle a physical ballot.

b) Require counties and SOS to publicly post the Numbered Voters List for each election

Said chapter is amended in Code Section 21-2-456, relating to posting of the electors who voted list as follows:

(b) Immediately upon the completion of the count and tabulation of the vote cast, the hand written paper electors list shall be sealed and returned immediately by the chief manager to the superintendent, who shall immediately post the list on the county web site or at the election office and transmit it to the registrars.

c) Require counties and SOS to publicly post the Eligible Electors List for each election

Said chapter is amended in Code Section 21-2-401, relating to posting of the certified electors lists as follows:

"The registrars shall, prior to the hour appointed for opening the polls, post on the county web site or at the office and place in the possession of the managers in each precinct one copy of the **certified electors list** for such precinct, such list to contain all the information required by law. …"

d) Establish a fully independent SEB to handle election investigations more appropriately

Said title is further amended by revising Code Section 21-2-31, relating to the authority and duties of the State Election Board, as follows:

“~~It shall be the duty of the~~ The State Election Board shall have the authority and be adequately funded to perform its duties:

(1) To ~~promulgate rules and regulations~~ supervise and coordinate the work of the office of the Secretary of State, superintendents, registrars, deputy registrars, poll officers, and other officials so as to obtain uniformity in the practices and proceedings ~~of superintendents, registrars, deputy registrars, poll officers, and other officials,~~ as well as the legality and purity in all primaries and elections;

(2) To formulate, adopt, and promulgate ~~such~~ rules and regulations, consistent with law, as will be conducive to the fair, legal, and orderly conduct of primaries and elections; and, upon the adoption of each rule and regulation, the board shall promptly file certified copies thereof with the Secretary of State and each superintendent;

(3) To publish in print or electronically and furnish to primary and election officials, from time to time, a sufficient number of indexed copies of all primary and election laws and pertinent rules and regulations then in force;

(4) To publish in print or electronically and distribute such explanatory pamphlets regarding the interpretation and application of primary and election laws as in the opinion of the board should be distributed to the electorate;

(5) To investigate~~, or authorize the Secretary of State to investigate,~~ when necessary or advisable the administration of primary and election laws and frauds and irregularities in primaries and elections and to report violations of the primary and election laws either to the Attorney General or the appropriate district attorney who shall be responsible for further investigation and prosecution. Nothing in this paragraph shall be so construed as to require any complaining party to request an investigation by the board before such party might proceed to seek any other remedy available to that party under this chapter or any other provision of law;

(6) To maintain legal custody of all state election documents, investigative reports, other election records, and communications between the Secretary of State and superintendents.

~~**(6)**~~ **(7)** To make such recommendations to the General Assembly as it may deem advisable relative to the conduct and administration of primaries and elections;

~~**(7)**~~ **(8)** To promulgate rules and regulations to define uniform and nondiscriminatory standards concerning what constitutes a vote and what will be counted as a vote for each category of voting system used in this state;

(9) To perform evaluations and selections of new voting system equipment, voter registration systems, electronic poll book systems, election results publishing systems and other election related systems as needed from time to time by the state and to identify when use of any such system shall be terminated;

~~**(8)**~~ **(10)** To employ investigators, attorneys and administrative staff ~~such~~ ~~assistants~~ as ~~may be~~ necessary to fully carry out its duties;

~~(9)~~ **(11)** Subject to funds being specifically appropriated by the General Assembly, to formulate and conduct a voter education program concerning voting procedures for voting by absentee ballot and at the polls with particular emphasis on the proper types of identification required for voting; and

~~(10)~~ **(12)** To take such other action, consistent with law, as the board may determine to be conducive to the fair, legal, and orderly conduct of primaries and elections.

e) Establish an Election Court for timely unbiased processing of election cases

Producing bill language for an election court exceeds the scope of capabilities for VoterGA. Possible language that could be used to draft an Election Court bill could include:

Whereby it is in the interests of the citizens and State of Georgia to have representation on matters pertaining to the interpretation of Georgia's Election Code and uniformity in the interpretation of Georgia's Election Code and the conduct of elections within the State of Georgia, thereby increasing Georgia's citizen's confidence that "judge shopping" does not occur in order to attempt to improperly influence Georgia's elections.

Therefore, pursuant to Article 6 of the Georgia Constitution, The Georgia Statewide Business Court shall create a division known as "The Georgia Statewide Election Court" which shall be the exclusive jurisdiction and venue for all matters under and related to O.C.G.A. Title 21, including but not limited to the Georgia State Election Board, election contests, and the conduct of all elections in the State of Georgia.

The Georgia Statewide Election Court shall be exclusively comprised of retired Superior Court Judges from each of Georgia's judicial circuits. No appointed or currently elected superior court judge shall be eligible to serve on The Georgia Statewide Election Court. Each of Georgia's judicial circuits, via the Chief Judge of the Circuit, shall appoint two retired eligible Superior Court Judges to this Court for a two-year term beginning July 1st. In the event of a death, withdrawal, or vacancy, the Chief Judge of the Superior Circuit whereby a vacancy occurred shall appoint a replacement retired superior court judge within 30 calendar days of the vacancy occurring to fill the remainder of the vacant term.

All matters before The Georgia Statewide Election Court shall be heard by a three-judge panel selected at random by the clerk of Court. No judge shall be eligible to hear a matter that is from a judicial circuit whereby a party in the suit resides. No judicial circuit shall have more than one superior court judge hearing the same case. In the event that the State of Georgia, the State Election Board, a statewide office or candidate, or a U.S. Senate candidate or race, or a Presidential candidate or race, or the conduct of an election for any of the aforementioned offices is at issue before The Georgia Statewide Election Court, then three judge panel shall be comprised of any of The Georgia Statewide Election Court judges so long as not more than one judge from a judicial circuit hears the case.

The Georgia Civil Practice Act shall be applied in all matters before The Georgia Statewide Election Court and a majority opinion shall be rendered at the most expeditious pace possible while maintaining fairness, justice, and impartiality. All cases before The Georgia Statewide Election Court shall be appealable via direct appeal to the Supreme Court of Georgia.

2. BALLOT SECURITY

a) Provide unique ballot identifiers to help prevent and detect unauthorized duplication

Said chapter is amended in Code Section 21-2-372, relating to the description of ballots as follows:

21-2-372. Ballot description; watermark required, unique ID required.
Ballots shall be of suitable design, size, and stock to permit processing by a ballot scanner and shall be printed in black ink on clear, white, or colored material. Other than ballots delivered electronically to qualified electors who are entitled to vote by absentee ballot under the federal Uniformed and Overseas Citizens Absentee Voting Act, 52 U.S.C. Section 20301, et seq., the ballots shall be printed on security paper that incorporates features which can be used to authenticate <u>and uniquely identify</u> the ballot as an official ballot but which do not make the ballot identifiable to a particular elector, provided that at least one such feature is a visible watermark that identifies the ballot as an official Georgia ballot.

b) Require absentee voters to designate an identifiable deliverer to return their ballot

Said chapter is amended in Code Section 21-2-381, relating to making of application for absentee ballot; determination of eligibility by a ballot clerk as follows:
"21-2-381.
(a)
(1)
(A) Except as otherwise provided in Code Section 21-2-219 or for advance voting described in subsection (d) of Code Section 21-2-385, not earlier than 78 days or less than 11 days prior to the date of the primary or election, or runoff of either, in which the elector desires to vote, any absentee elector may make, either by mail, by facsimile transmission, by electronic transmission, or in person in the registrar's or absentee ballot clerk's office, an application for an official ballot of the elector's precinct to be voted at such primary, election, or runoff. To be timely received, an application for an absentee-by-mail ballot shall be received by the board of registrars or absentee ballot clerk no later than 11 days prior to the primary, election, or runoff. For advance voting in person, the application shall be made within the time period set forth in subsection (d) of Code Section 21-2-385.
(B) In the case of an elector residing temporarily out of the county or municipality or a physically disabled elector residing within the county or municipality, the application for the elector's absentee ballot may, upon satisfactory proof of relationship, be made by such elector's mother, father, grandparent, aunt, uncle, sister, brother, spouse, son, daughter, niece, nephew, grandchild, son-in-law, daughter-in-law, mother-in-law, father-in-law, brother-in-law, or sister-in-law of the age of 18 or over.
(C)
(i) Any person applying for an absentee-by-mail ballot shall make application in writing on the form made available by the Secretary of State. In order to confirm the identity of the voter, such form shall require the elector to provide his or her name, date of birth, address as registered, address where the elector wishes the ballot to be mailed, and the number of his or her Georgia driver's license or identification card issued pursuant to Article 5 of Chapter 5 of Title 40. If such elector does not have a Georgia driver's license or identification card issued pursuant to Article 5 of Chapter 5 of Title 40, the elector shall affirm this fact in the manner prescribed in the application and the elector shall provide a copy of a form of identification

listed in subsection (c) of Code Section 21-2-417. The elector shall provide the name and address of up to three designated deliverers, any one of whom may deliver the elector’s voted absentee ballot sealed in the envelope provided with the ballot to the county election office or other location designated by the county election office to receive such voted absentee ballots. The form made available by the Secretary of State shall include a space to affix a photocopy or electronic image of such identification. The Secretary of State shall develop a method to allow secure electronic transmission of such form. The application shall also include the identity of the primary, election, or runoff in which the elector wishes to vote; the name and relationship of the person requesting the ballot if other than the elector; and an oath for the elector or relative to write his or her usual signature with a pen and ink affirming that the elector is a qualified Georgia elector and the facts presented on the application are true. Submitting false information on an application for an absentee ballot shall be a violation of Code Sections 21-2-560 and 21-2-571.

(ii) A blank application for an absentee ballot shall be made available online by the Secretary of State and each election superintendent and registrar, but neither the Secretary of State, election superintendent, board of registrars, other governmental entity, nor employee or agent thereof shall send absentee ballot applications directly to any elector except upon request of such elector or a relative authorized to request an absentee ballot for such elector. No person or entity other than a relative authorized to request an absentee ballot for such elector or a person signing as assisting an illiterate or physically disabled elector shall send any elector an absentee ballot application that is prefilled with the elector’s required information set forth in this subparagraph. No person or entity other than the elector, a relative authorized to request an absentee ballot for such elector, a person signing as assisting an illiterate or physically disabled elector with his or her application, a common carrier charged with returning the ballot application, an absentee ballot clerk, a registrar, or a law enforcement officer in the course of an investigation shall handle or return an elector’s completed absentee ballot application. Handling a completed absentee ballot application by any person or entity other than as allowed in this subsection shall be a misdemeanor. Any application for an absentee ballot sent to any elector by any person or entity shall utilize the form of the application made available by the Secretary of State and shall clearly and prominently disclose on the face of the form:
“This application is being distributed by [insert name and address of person, organization, or other entity distributing such document or material], not by any government agency or any state or local election office. THIS IS NOT A BALLOT.”

c) Replace mail-in voting with identified, designated ballot deliverers

Said chapter is amended in Code Section 21-2-385, relating to delivery and acceptance of absentee ballots as follows’

″21-2-385.

(a) At any time after receiving an official absentee ballot, but before the day of the primary or election, except electors who are confined to a hospital on the day of the primary or election, the elector shall vote his or her absentee ballot, then fold the ballot and enclose and securely seal the same in the envelope on which is printed "Official Absentee Ballot." This envelope shall then be placed in the second one, on which is printed the form of the oath of the elector; the name and oath of the person assisting, if any; and other required identifying information. The elector shall then fill out, subscribe, and swear to the oath printed on such envelope. In order to verify that the absentee ballot was voted by the elector who requested the ballot, the elector shall print the number of his or her Georgia driver's license number or identification card issued pursuant to Article 5 of Chapter 5 of Title 40 in the space provided on the outer oath envelope. The elector shall also print his or her date of birth in the space provided in the outer oath envelope. If the elector does not have a Georgia driver's license or state identification card issued pursuant to Article 5 of Chapter 5 of Title 40, the elector shall so affirm in the space provided on the outer oath envelope and print the last four digits of his or her social security number in the space provided on the outer oath envelope. If the elector does not have a Georgia driver's license, identification card issued pursuant to Article 5 of Chapter 5 of Title 40, or a social security number, the elector shall so affirm in the space provided on the outer oath envelope and place a copy of one of the forms of identification set forth in subsection (c) of Code Section 21-2-417 in the outer envelope. Such envelope shall then be securely sealed and the elector shall then personally give the envelope to their designated deliverer who shall ~~mail or~~ personally deliver same and show identification to the board of registrars or absentee ballot clerk~~, provided that mailing or delivery may be made by the elector's mother, father, grandparent, aunt, uncle, brother, sister, spouse, son, daughter, niece, nephew, grandchild, son-in-law, daughter-in-law, mother-in-law, father-in-law, brother-in-law, sister-in-law, or an individual residing in the household of such elector~~. The absentee ballot of a disabled elector may be ~~mailed or~~ delivered by the caregiver of such disabled elector, regardless of whether such caregiver resides in such disabled elector's household provided that the caregiver has been designated as a deliverer and shows identification upon delivery. The absentee ballot of an elector who is in custody in a jail or other detention facility may be ~~mailed or~~ delivered by any employee of such jail or facility having custody of such elector provided that the employee has been designated as a deliverer and shows identification upon delivery. An elector who is confined to a hospital on a primary or election day to whom an absentee ballot is delivered by the registrar or absentee ballot clerk shall then and there vote the ballot, seal it properly, and return it to the registrar or absentee ballot clerk. If the elector registered to vote for the first time in this state by mail and has not previously provided the identification required by Code Section 21-2-220 and votes for the first time by absentee ballot and fails to provide the identification required by Code Section 21-2-220 with such absentee ballot, such absentee ballot shall be treated as a provisional ballot and shall be counted only if the registrars are able to verify the identification and registration of the elector during the time provided pursuant to Code Section 21-2-419.

d) Track delivery of all absentee ballots mailed to voters

Said chapter is amended in Code Section 21-2-384, relating to delivery and acceptance of absentee ballots as follows:'
"21-2-384.
(a)

(1) The superintendent shall, in consultation with the board of registrars or absentee ballot clerk, prepare, obtain, and deliver before the date specified in paragraph (2) of this subsection an adequate supply of official absentee ballots to the board of registrars or absentee ballot clerk for use in the primary or election or as soon as possible prior to a runoff. Envelopes and other supplies as required by this article may be ordered by the superintendent, the board of registrars, or the absentee ballot clerk for use in the primary or election.

(2) The board of registrars or absentee ballot clerk shall mail or issue official absentee ballots using a USPS or third-party tracking system to all eligible applicants not more than 29 days but not less than 25 days prior to any presidential preference primary, general primary other than a municipal general primary, general election other than a municipal general election, or special primary or special election in which there is a candidate for a federal office on the ballot; 22 days prior to any municipal general primary or municipal general election; and as soon as possible prior to any runoff. In the case of all other special primaries or special elections, the board of registrars or absentee ballot clerk shall mail or issue official absentee ballots to all eligible applicants within three days after the receipt of such ballots and supplies, but no earlier than 22 days prior to the election; provided, however, that official absentee ballots shall be issued to any elector of the jurisdiction who is entitled to vote by absentee ballot under the federal Uniformed and Overseas Citizen Absentee Voting Act, 52 U.S.C. Section 20301, et seq., as amended, beginning 49 days prior to a federal primary or election and not later than 45 days prior to a federal primary or election. As additional applicants who submitted timely applications for an absentee ballot are determined to be eligible, the board or clerk shall mail or issue official absentee ballots to such additional applicants immediately upon determining their eligibility. For all timely received applications for absentee ballots, the board of registrars or absentee ballot clerk shall mail or issue absentee ballots, provisional absentee ballots, and notices of rejection as soon as possible upon determining their eligibility within the time periods set forth in this subsection. During the period for advance voting set forth in Code Section 21-2-385, the board of registrars or absentee ballot clerk shall make such determinations and mail or issue absentee ballots, provisional absentee ballots, and notices of rejection of application within three days after receiving a timely application for an absentee ballot. The board of registrars or absentee ballot clerk shall, within the time periods specified in this subsection, electronically transmit official absentee ballots to all electors who have requested to receive their official absentee ballot electronically and are entitled to vote such absentee ballot under the federal Uniformed and Overseas Citizens Absentee Voting Act, 52 U.S.C. Section 20301, et seq., as amended

e) Require counties to accept all absentee ballots including UOCAVA ballots by Election Day

Said chapter is amended in Code Section 21-2-386, relating to the time for acceptance of absentee ballots as follows:

"21-2-386.

“(A) The board of registrars or absentee ballot clerk shall keep safely, unopened, and stored in a manner that will prevent tampering and unauthorized access to and shall document authorized access to all official absentee ballots received from absentee electors prior to Election Day ~~the closing of the polls on the day~~ of the primary or election except as otherwise provided in this subsection.”

(B) Upon receipt of each ballot, a registrar or clerk shall write the day and hour of the receipt of the ballot on its envelope. The registrar or clerk shall then compare the number of the elector's Georgia driver's license number or state identification card issued pursuant to Article 5 of Chapter 5 of Title 40 and date of birth entered on the absentee ballot envelope with the same information contained in the elector's voter registration records. If the elector has affirmed on the envelope that he or she does not have a Georgia driver's license or state identification card issued pursuant to Article 5 of Chapter 5 of Title 40, the registrar or clerk shall compare the last four digits of the elector's social security number and date of birth entered on the envelope with the same information contained in the elector's voter registration records. The registrar or clerk shall also confirm that the elector signed the oath and the person assisting the elector, if any, signed the required oath. If the elector has signed the elector's oath, the person assisting has signed the required oath, if applicable, and the identifying information entered on the absentee ballot envelope matches the same information contained in the elector's voter registration record, the registrar or clerk shall so certify by signing or initialing his or her name below the voter's oath. Each elector's name so certified shall be listed by the registrar or clerk on the numbered list of absentee voters prepared for his or her precinct. All accepted absentee ballots shall be securely stored in either a sealed container or appropriately secured in an access controlled room that will prevent tampering or unauthorized access prior to the scanning of such ballots.

(C) If the elector has failed to sign the oath, or if the identifying information entered on the absentee ballot envelope does not match the same information appearing in the elector's voter registration record, or if the elector has failed to furnish required information or information so furnished does not conform with that on file in the registrar's or clerk's office, or if the elector is otherwise found disqualified to vote, the registrar or clerk shall write across the face of the envelope "Rejected," giving the reason therefor. The board of registrars or absentee ballot clerk shall promptly notify the elector of such rejection, a copy of which notification shall be retained in the files of the board of registrars or absentee ballot clerk for at least two years. Such elector shall have until the end of the period for verifying provisional ballots contained in subsection (c) of Code Section 21-2-419 to cure the problem resulting in the rejection of the ballot. The elector may cure a failure to sign the oath, nonmatching identifying information, or missing information by submitting an affidavit to the board of registrars or absentee ballot clerk along with a copy of one of the forms of identification enumerated in subsection (c) of Code Section 21-2-417 before the close of such period. The affidavit shall affirm that the ballot was submitted by the elector, is the elector's ballot, and that the elector is registered and qualified to vote in the primary, election, or runoff in question. If the board of registrars or absentee ballot clerk finds the affidavit and identification to be sufficient, the absentee ballot shall be counted.

(D) An elector who registered to vote by mail, but did not comply with subsection (c) of Code Section 21-2-220, and who votes for the first time in this state by absentee ballot shall include with his or her application for an absentee ballot or in the outer oath envelope of his or her absentee ballot either one of the forms of identification listed in subsection (a) of Code Section 21-2-417 or a copy of a current utility bill, bank statement, government check, paycheck, or other government document that shows the name and address of such elector. If such elector does not provide any of the forms of identification listed in this subparagraph with his or her application for an absentee ballot or with the absentee ballot, such absentee ballot shall be deemed to be a provisional ballot and such ballot shall only be counted if the registrars are able to verify current and valid identification of the elector as provided in this subparagraph within the time period for verifying provisional ballots pursuant to Code Section 21-2-419. The board of registrars or absentee ballot clerk shall promptly notify the elector that such ballot is deemed a provisional ballot and shall provide information on the types of identification needed and how and when such identification is to be submitted to the board of registrars or absentee ballot clerk to verify the ballot.

(E) Three copies of the numbered list of voters shall also be prepared for such rejected absentee electors, giving the name of the elector and the reason for the rejection in each case. Three copies of the numbered list of certified absentee voters and three copies of the numbered list of rejected absentee voters for each precinct shall be turned over to the poll manager in charge of counting the absentee ballots and shall be distributed as required by law for numbered lists of voters.

(F) All absentee ballots returned to the board or absentee ballot clerk after the closing of the polls on the day of the primary or election shall be safely kept unopened by the board or absentee ballot clerk and then transferred to the appropriate clerk with the documentation provided for in subparagraph (a)(1)(A) of this Code section for storage in a manner that will prevent tampering for the period of time required for the preservation of ballots used at the primary or election and shall then, without being opened, be destroyed in like manner as the used ballots of the primary or election. The board of registrars or absentee ballot clerk shall promptly notify the elector by first-class mail that the elector's ballot was returned too late to be counted and that the elector will not receive credit for voting in the primary or election. All such late absentee ballots shall be delivered to the appropriate clerk and stored as provided in Code Section 21-2-390.

~~(G) Notwithstanding any provision of this chapter to the contrary, until the United States Department of Defense notifies the Secretary of State that the Department of Defense has implemented a system of expedited absentee voting for those electors covered by this subparagraph, absentee ballots cast in a primary, election, or runoff by eligible absentee electors who reside outside the county or municipality in which the primary, election, or runoff is held and are members of the armed forces of the United States, members of the merchant marine of the United States, spouses or dependents of members of the armed forces or merchant marine residing with or accompanying such members, or overseas citizens that are postmarked by the date of such primary, election, or runoff and are received within the three-day period following such primary, election, or runoff, if proper in all other respects, shall be valid ballots and shall be counted and included in the certified election results.~~

f) Allow for Ballot on Demand printing to replace unverifiable BMDs

SB214 as passed in the Senate provides language to accommodate BOD printing and requires simple modifications for proposed unique ballot IDs and to adjust for the fact that the EAC does not separately certify BOD printers. The SB214 language included here is not intended to override language otherwise provided by SB303. The proposed SB214 language changes are shown in red below:

SECTION 1.

Chapter 2 of Title 21 of the Official Code of Georgia Annotated, relating to elections and primaries generally, is amended in Code Section 21-2-2, relating to definitions, by adding a new paragraph to read as follows:

"(2.05) 'Ballot on demand printing' means a stand-alone system that prints uniquely identified ballots for each ballot style within a county or municipality."

SECTION 2.

Said chapter is further amended by revising Code Section 21-2-300, relating to provision of new voting equipment by state, uniform system using ballot scanners, pilot programs, county obligations, and use of physical ballots, as follows:

"21-2-300.
(a)(1) The equipment used for casting and counting votes in county, state, and federal elections shall 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.

(2) As soon as possible, once such equipment is certified by the Secretary of State as safe and practicable for use, all federal, state, and county general primaries and general elections as well as special primaries and special elections in the State of Georgia shall be conducted with the use of ~~scanning ballots marked by electronic ballot markers and~~ an optical scanning voting system utilizing nonelectronic ballot markers and ballot on demand printing, and shall be tabulated by using ballot scanners that also create scanned images of tabulated ballots, for voting at the polls and for absentee ballots cast in person, unless otherwise authorized by law; provided, however, that such ~~electronic ballot markers~~ system shall produce paper ballots which are marked with the elector's choices in a format readable by the elector.

(3) The state shall furnish a uniform optical scanning voting system and ballot on demand printing system of ~~electronic ballot markers and~~ ballot scanners for use in each county as soon as possible. Such optical scanning voting system equipment shall be certified by the United States Election Assistance Commission prior to purchase, lease, or acquisition. At its own expense, the governing authority of a county may purchase, lease, or otherwise acquire additional ~~electronic ballot markers~~ optical scanning voting and ballot on demand printing equipment and ballot scanners of the type furnished by the state, if the governing authority so desires. Additionally, at its own expense, the governing authority of a municipality may choose to acquire its own ~~electronic ballot markers~~ optical scanning voting system, ballot on demand printing equipment, and ballot scanners by purchase, lease, or other procurement process.

(4) Notwithstanding any provision of law to the contrary, the Secretary of State is authorized to conduct pilot programs to test and evaluate the use of ~~electronic ballot markers~~ an optical scanning voting system, ballot on demand printing, and ballot scanners in primaries and elections in this state. (b) Each county shall, prior to being provided with voting equipment by the state, provide polling places that are adequate for the operation of such equipment including, if necessary, the placement within the polling places of a sufficient number of electrical outlets and telephone lines.

(c) Each county shall, prior to being provided with voting equipment by the state, provide or contract for adequate technical support for the installation, set up, and operation of such voting equipment for each primary, election, and special primary and special election as the Secretary of State shall determine by rule or regulation.

(d) The Secretary of State shall be responsible for the development, implementation, and provision of a continuing program to educate voters, election officials, and poll workers in the proper use of such voting equipment. Each county shall bear the costs, including transportation, subsistence, and lodging, incurred by its election and registration officials in attending courses taught by or arranged by the Secretary of State for instruction in the use of the voting equipment.

(e)(1) Counties shall be authorized to contract with municipal governments for the use of such voting equipment in municipal elections under terms and conditions specified by the Secretary of State to assure that the equipment is properly used and kept secure.

(2) Notwithstanding the provisions of Code Section 21-2-45, counties may not levy a fee for use of state-owned voting equipment but may require municipalities to reimburse the county for the actual expenses related to the election or elections that are subject to the county and municipal contract.

~~(f)(1) Notwithstanding any provision of this Code section to the contrary, provided that the county election superintendent has petitioned and received the approval of the State Election Board at least 10 days prior to the beginning of advance voting, in any election with less than 5,000 registered electors, such superintendent may provide the electors physical ballots on the same type of ballot that is used for absentee ballots pursuant to subsection (a) of Code Section 21-2-383 and allow electors to mark their ballot using a pen, pencil, or similar non-electronic writing tool as an alternative to using electronic ballot marking devices.~~
~~(2) Such physical ballots may only be used to conduct:~~

~~(A) Special primaries, special elections, or runoffs thereof for county offices; or~~
~~(B) Special elections to present a question to the voters of a county.~~

~~Furthermore, such primary, special primary, election, or special election shall occur independently and apart from a presidential preference primary, state-wide general primary, state-wide special primary, state-wide general election, or state-wide special election."~~

3. VOTER DATA SECURITY

a) Ensure only those who proactively choose to register through DDS can Opt-in to vote

Said chapter is amended in Code Section 21-2-221.1 relating to registration of voters

(a) Each application to obtain a obtain, renew, or change the name or address on a driver's license or identification card issued by the Department of Driver Services pursuant to Chapter 5 of Title 40 made by an applicant who is within six months of such applicant's eighteenth birthday or older shall also serve as an application for voter registration ~~unless~~ if the applicant ~~declines~~ requests to register to vote through specific confirmation and signs ~~declination or by failing to sign~~ the voter registration application.

Said chapter is amended in Code Section 21-2-221 relating to registration of voters

(a) Each application to obtain a resident hunting, fishing, or trapping license issued by the Department of Natural Resources pursuant to Chapter 2 of Title 27 and made by an applicant who is within six months of such applicant's eighteenth birthday or older shall also serve as an application for voter registration ~~unless~~ if the applicant ~~declines~~ requests to register to vote through specific confirmation and signs ~~declination or by failing to sign~~ the voter registration application.

Said chapter is amended in Code Section 21-2-222 relating to registration of voters

(f)(2)(C) Boxes for the applicant to check to indicate whether the applicant is presently registered, or would like to register~~, or declines to register~~ to vote with the statement "IF YOU DO NOT CHECK ANY BOX, YOU WILL BE CONSIDERED TO HAVE DECIDED NOT TO REGISTER TO VOTE AT THIS TIME." in close proximity to the boxes and in prominent type;

(f)(3) Provide to each applicant who applies ~~does not decline to apply~~ to register to vote the same degree of assistance with regard to the completion of the voter registration application form as is provided by the office with regard to the completion of its own forms, unless the applicant refuses such assistance.

b) Verify voter eligibility and address accuracy

Said chapter is amended in Code Section 21-2-226, relating to eligibility of voters and accuracy of voter registration data as follows:

(a) It shall be the duty of the county board of registrars to determine the eligibility of each living person applying to register to vote in such county. The eligibility shall include verification of citizenship, age, valid county residential address, deliverable mailing address, passage of criminal background check and government issued photo identification.

c) Impose penalties on counties that refuse to properly maintain their voter rolls

Said chapter is amended in Code Section 21-2-230, relating to requirements for challenges of persons on lists of electors to impose penalties for failure to remove ineligible registrations as follows:

(j) Failure to comply with the provision of this Code section by the board of registrars shall subject such board to sanctions by the State Election Board and a penalty not less than $100 and not more than $1000 for each ineligible voter roll entry that the board fails to inactivate or cancel according to its duties defined in this Code Section ~~remove~~.

(k) No fee or reimbursement of costs shall be imposed on the elector submitting a challenge under this Code Section.

d) Require DDS address changes to be accurately applied to the voter roll database

Said chapter is amended in Code Section 21-2-221, relating to transmission of drivers' license address updates to the Secretary of State and to the county board of registrars as follows:

(i) The Department of Driver Services shall transmit all voter address updates to the Secretary of State at the conclusion of each business day. The Secretary of State shall forward each address update to the appropriate county board of registrars who shall ensure that the voter registration record is updated with the new address within 30 days and placed in the correct precinct and voting districts. The registrars will also assure that any prior registrations that may exist are cancelled.

e) Clearly prohibit 3rd party vendor involvement in Georgia voter roll data

Said chapter is amended in Code Section 21-2-211, relating to requirements to prohibit third party manipulation, transmission or control of voter data, timely publication of eligible electors list and numbered voters list at no charge as follows:

(a) The Secretary of State shall establish and maintain a list of all eligible and qualified registered electors to be housed on government-owned servers within ~~in~~ this state which shall be the official list of electors for use in all elections in this state conducted under this title.

(b)

(1) As used in this subsection, the term “equipment” shall include, but not be limited to, computer hardware; computer software; modems, controllers, and other data transmission devices; data transmission lines; scanners and other digital imaging devices; and printers under direct control of the office of the Secretary of State at all times.

(2) The Secretary of State is authorized to procure and provide all of the necessary equipment to permit the county boards of registrars to access and utilize the official list of electors maintained by the Secretary of State pursuant to this Code section, provided that funds are specifically appropriated by the General Assembly for that purpose. The Secretary of State shall maintain exclusive control of such equipment and such equipment shall be utilized only by state and local government officials or their employees without outsourcing of any administrative or technical functions other than standard technical support.

(3) The Secretary of State and county boards of registrars shall be the exclusive custodians of their official lists of electors which shall be maintained exclusively on state or county government-owned servers. The Secretary of State and county boards shall protect their official electors lists from being transmitted to, manipulated by, or controlled by any third-party vendor or non-governmental entity.

(4) The Secretary of State shall provide by procedure, rule, or regulation for the mechanism by which voter registration data identified in this Code Section and Code Section 21-2-225 as private, shall be kept confidential from third party vendors and non-governmental entities.

(5) The boards of registrars shall ensure that all eligible and qualified electors have been entered into the voter registration database and verified as eligible at least thirty days prior to each election. The boards and Secretary of State shall make their official lists of eligible and qualified electors publicly available at least five days prior to each election that is conducted at no charge. No additional electors shall be added to the voter rolls until seven days after the election is closed.

(6) The Secretary of State shall make a supplemental list of electors containing any changes made to the official eligible elector list data from the time it is published prior to the election until completion of the conduct of the election publicly available within three days after each election is conducted at no charge.

(7) The Secretary of State shall make the official list of eligible and qualified electors who voted in each election, also known as the numbered list of voters pursuant to O.C.G.A. § 21-2-456(a), and the full voter history data publicly available within three days after each election is conducted at no charge.