IN THE COURT OF APPEALS

STATE OF GEORGIA

DEKALB COUNTY REPUBLICAN PARTY, INC.,

APPELLANT,

v.

BRAD RAFFENSPERGER, IN HIS OFFICIAL CAPACITY AS THE SECRETARY OF STATE OF GEORGIA,

APPELLEE

Case No. A25A0831

BRIEF OF APPELLANT

CALDWELL, CARLSON, ELLIOTT & DELOACH, LLP

/s/ Harry W. MacDougald
Harry W. MacDougald
Ga. Bar No. 463076
6 Concourse Parkway
Suite 2400
Atlanta, Georgia 30328
(404) 843-1956
hmacdougald@ccedlaw.com

HARDING LAW FIRM, LLC

/s/ Todd A. Harding
Todd A. Harding, For the Firm
Ga. Bar No.: 101562
Attorney at Law
HARDING LAW FIRM, LLC
113 E. Solomon Street
Griffin, Georgia 30223
(770) 229-4578
(770) 228-9111 facsimile

Counsel for Appellant

TABLE OF CONTENTS

Table of Authorities iv

Introduction 1

Statement of Jurisdiction 3

Enumeration of Errors 3

Statement of The Case 3

I. Material Facts Relevant to Appeal 3

II. Statement of Proceedings Below 12

III. Method of Preservation of Error 14

Summary of Argument 15

Argument and Citation of Authority 17

I. The Nature and Elements of Mandamus Relief 17

II. The Cybersecurity Requirements Incorporated into the Certification Required by O.C.G.A. § 21-2-300(a) 19

III. O.C.G.A. § 21-2-300(a) Should be Construed to Require Compliance with EAC Cybersecurity Standards in the Operational Context. 22

1. The Text 22

2. The Rules of Construction 23

3. Application of the Rules of Construction 27

a. Textual analysis. 27

b. Legal Context 28

c. EAC testing program documents require ongoing compliance with certification standards. 30

d. FIPS 140-2 requires operational compliance. 32

e. Modifications to ensure continuing compliance are managed through engineering change orders. 33

f. The Secretary's contract with the system vendor requires operational compliance. 33

g. A Predecessor Secretary of State contended that insecure encryption keys were a serious security issue. 36

4. History Leading to Adoption of O.C.G.A. § 21-2-300. 38

IV. The Secretary has Breached his Duty to Ensure that Georgia's Election Systems Comply with the Applicable Certification Requirements. 40

Conclusion 42

TABLE OF AUTHORITIES

Cases

Bellsouth Telecommunications, LLC v. Cobb Cnty.,
305 Ga. 144 (2019) 25

Bellsouth Telecommunications, LLC v. Cobb County,
342 Ga. App. 323 (2017) 25

Bibb Cnty. v. Monroe Cnty.,
294 Ga. 730 (2014) 18

Chan v. Ellis,
296 Ga. 838 (2015) 24

Citizens' Bank of Folkston, etc. v. Newton,
180 Ga. 860 (1935) 19

Curling v. Raffensperger,
493 F. Supp. 3d 1264 (N.D. Ga. 2020) 32, 37

Deal v. Coleman,
294 Ga. 170 (2013)) 24

FDIC v. Loudermilk,
305 Ga. 558 (2019) 24, 25, 28

Gaw v. Telfair Cnty. Bd. of Comm'rs,
277 Ga. 157 (2003) 18

Giller v. Slosberg,
359 Ga. App. 867 (2021) 26

Hartley v. Agnes Scott College,
295 Ga. 458 (2014) 21

Kingdom Retail Grp., LLC v. Pandora Franchising, LLC,
334 Ga. App. 812 (2015) 4

Love v. Fulton Cnty. Bd. of Tax Assessors,
311 Ga. 682 (2021) 17, 18

Patton v. Vanderpool,
302 Ga. 253 (2017) 25

Slosberg v. Giller,
314 Ga. 89 (2022) 27

Smith v. DeKalb Cnty.,
288 Ga. App. 574 (2007) 36

Sons of Confederate Veterans v. Henry County Board of Commissioners,
315 Ga. 39 (2022) 17

State v. Henderson,
263 Ga. 508 (1993) 21

Undercofler v. Scott,
220 Ga. 406 (1964) 19

Weathers v. Easterling,
153 Ga. 60 (1922) 19

Zaldivar v. Prickett,
297 Ga. 589 (2015) 24

Statutes

52 U.S.C. § 21081 22

52 U.S.C. § 21101 21

O.C.G.A. § 1-3-1 ..... 23, 25, 39

O.C.G.A. § 15-3-3.1 3

O.C.G.A. § 21-2-300 ..... passim

O.C.G.A. § 21-2-324 ..... 2, 4, 41

O.C.G.A. § 21-2-50.2 21

O.C.G.A. § 24-2-201 4

O.C.G.A. § 51-12-33 25

O.C.G.A. § 9-6-20 17

O.C.G.A. § 9-6-21 ..... 17, 18

O.C.G.A. § 9-6-28 17

Treatises

Blackstone's COMMENTARIES ON THE LAWS OF ENGLAND (1st ed. 1768) 24

Other References

Beth K. Boatright and Andrew Smith, *HB 316 - Voting System*, 36 GEORGIA STATE U. L. REV. 81. (2019) 38

Charles M. Cork, III, *Reading Law in Georgia* 26

John F. Manning, *The New Purposivism*, 2011 SUP. CT. REV. 113 26

Jonathan T. Molot, *The Rise and Fall of Textualism*, 106 COLUM. L. REV. 1, 2–3 (2006) 26

Peter Loshin, *What is an encryption key?* TECHTARGET 5

Tim Mucci, *What is structured query language (SQL)?,* IBM, ... 11

WORDNIK 5

INTRODUCTION

The issue in this mandamus case is whether it is unlawful for the Secretary of State to require Georgia counties to use election systems that the overwhelming and uncontradicted evidence shows are grossly non-compliant with the cybersecurity standards of their certification. The trial court dismissed the application on the grounds that O.C.G.A. § 21-2-300 imposes no requirement that the systems comply with their cybersecurity certification requirements during their actual use in elections, the only context in which cybersecurity actually matters. Instead, the trial court held that the certification obligations of the statute were fully discharged if, prior to purchase or use, the systems were certified by the U.S. Election Assistance Commission ("EAC") and the Secretary, which they were. Based on its interpretation of the statute, the trial court dismissed the case despite the Secretary being on notice since July of 2021 of the grave security defect at issue in this case and doing literally nothing to fix it since then.

The statute, O.C.G.A. § 21-2-300, requires in subsection (a)(1) that the Secretary of State furnish election equipment to all Georgia counties for use in elections. Subsection (a)(2) requires that, upon the Secretary's certification of "such machines" "as safe and practicable ***for use***," all

elections "shall be conducted" using them. Subsection (a)(3) requires that the machines "shall be certified by the United States Election Assistance Commission prior to purchase, lease, or acquisition." Significantly, the Secretary has statutory discretion to revisit the ongoing safety of election equipment, O.C.G.A. § 21-2-324(a), and mandamus in Georgia extends to gross abuses of discretion.

The DeKalb County Republican Party, Inc. ("DeKalb GOP") sought mandamus relief against the Secretary of State because the election system used in Georgia does not meet the mandatory requirements of state law for certification and use in Georgia elections with respect to cybersecurity. The undisputed evidence showed in overwhelming fashion that the cybersecurity of these systems as used in Georgia elections is gravely deficient and fails to comply with the certification requirements, despite their actually having been certified before they were purchased.

After a full-day evidentiary hearing at which the State presented no evidence, the trial court granted the Secretary's motion to dismiss. The trial court's interpretation of the statute is erroneous and should be reversed. It turns the law of statutory interpretation on its head and imposes a result that

deprives Georgians of the secure election systems the plain text of the statute obviously requires.

STATEMENT OF JURISDICTION

The Court of Appeals has jurisdiction over this appeal pursuant to the timely filing of a Notice of Appeal and because jurisdiction is not expressly conferred upon the Supreme Court. O.C.G.A. § 15-3-3.1(a)(4).

ENUMERATION OF ERRORS

1. The trial court erred in dismissing the application for a writ of mandamus.

2. The trial court erred in its interpretation of the certification requirements of O.C.G.A. § 21-2-300(a)(2) and (3).

3. Even if the trial court did not err in interpreting the certification requirements, the Secretary grossly abused his discretion in failing to reexamine the election system's compliance with Georgia and federal law.

STATEMENT OF THE CASE

I. MATERIAL FACTS RELEVANT TO APPEAL

Georgia's election systems were certified by the EAC on January 30, 2019, prior to their purchase by the State. R5-347. *See* O.C.G.A. § 21-2-300(a)(3) (requiring pre-purchase EAC certification).

Per O.C.G.A. § 21-2-300(a)(2), the Secretary certified the election system as "safe and practicable for use" on August 9, 2019, again prior to purchase. His certificate states in pertinent part that:

> [T]he Dominion Voting System ... has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code and Rules of the Secretary of State, and as a result of this inspection. it is my opinion that this kind of voting system and its components can be ***safely used by the electors of this state in all primaries and elections*** as provided in Chapter 2 of Title 21 of the Official Code of Georgia; provided however, that I hereby reserve my opinion to ***reexamine this voting system and its components at any time so as to ensure that it continues to be one that can be safely used by the voters of this state***.[1]

(Emphasis added); *see also* O.C.G.A. § 21-2-324(a) (reserving Secretary's discretion to reexamine election systems).

The evidence showed without contradiction that the system does not in fact comply with EAC certification requirements for cybersecurity. In light of that, the Secretary's certification that the system was "safe and practicable for ***use***" is at best a grim irony, for it is simply not true. The system was

---

[1] Although the Secretary's certificate was not included in the record in Superior Court, it is undisputed that he did so certify the system, and the Secretary of State's records are judicially noticeable, *Kingdom Retail Grp., LLC v. Pandora Franchising, LLC*, 334 Ga. App. 812, 817 n.4 (2015), even on appeal. O.C.G.A. § 24-2-201(f).

certified as compliant with the applicable standards, but "in use" they are not, and there are no two ways about it. As more particularly detailed below, the evidence showed this in the following respects: (1) encryption keys[2] are stored in plaintext[3] in the election database; (2) the systems still have a hard-coded vendor password that grants administrative privileges that has been publicly known since 2010 at the latest, "dvscorp08!"; and (3) multiple users use the same usernames and passwords. These are all grave and appalling security vulnerabilities because they leave the system wide open to hacking and altering election results without detection.

Plaintiff presented back-up copies of election databases obtained from three Georgia counties through Open Records Act requests that were then

---

[2] "In cryptography, an encryption key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the text in a given message." Peter Loshin, *What is an encryption key?* TECHTARGET, https://www.techtarget.com/searchsecurity/definition/key (last visited Jan. 10, 2025).

[3] "Plaintext" in this context means the information is unencrypted and human-readable. *See* definition at WORDNIK, https://www.wordnik.com/words/plaintext (last visited Jan. 10, 2025).

analyzed by Plaintiff's experts.[4] Plaintiff's cybersecurity expert Clay Parikh used these back-up databases to testify and present a demonstrative video in which he showed and proved the following without contradiction:

- The machines can accessed by getting past the windows log on, a trivial barrier to even minimally experienced hackers. R5-90[5]; R5-198;
- The election software can be accessed by use of the hard-coded vendor password, dvscorp08!, which grants administrative user access to the election system, all election data, and stored user names and passwords, and is a vulnerability that was documented by a testing lab in 2010. R5-127-131; R5-133-136;
- Using the encryption keys, the results of an election could be altered in an ***undetectable manner.*** R5-115; R5-131 – R5-140.

---

[4] These election database backup files were admitted as Exh. 25, 26 and 27, R4-9; R5-244, but were not transmitted with the record to this Court because of the enormous file sizes – multiple gigabytes – and because they would be totally unreadable by the Court without the Dominion election software system. *See* Third Amended Notice of Appeal, R2-1.

[5] Record citations are to the pdf page number of the Volume the record per Court of Appeals Rule 25(d)(2).

- The existence in the database of multiple common usernames and passwords, R5-141-142, all visible with the administrative credentials granted by the hard-coded vendor password dvscorp08!, a vulnerability documented in lab testing in 2010. Exh. 31, R5-658.

Mr. Parikh characterized these flaws as "egregious," R5-113, R5-118, R5-159, R5-119, R5-130, and testified that the system was wide open to attack and manipulation of the results that could not be detected. R5-115-116, R5-140. He explained that the level of sophistication required to successfully hack the systems and change results without detection was not high, and would be a "cake walk" for a nation state adversary like China. R5-197-199.

Mr. Parikh also testified to his experience working in one of the voting system testing laboratories relied upon by the EAC to carry out certification testing of systems like Georgia's. R5-79. As a result, he was intimately familiar with the requirements of the Voluntary Voting System Guidelines ("VVSG") (Exh. 19 at R5-358), the benchmark for EAC certification testing. R5-77-79. In other words, to receive EAC certification, an election system has to meet the standards of the VVSG. R5-701; Exh. 16, R5-340. Mr. Parikh identified the sections of the VVSG that impose standards for cybersecurity,

and explained that they incorporate a federal cybersecurity standard known as Federal Information Protection Standards 140-2 ("FIPS 140-2") (Exh. 20, R5-582). R-95-97. FIPS 140-2 imposes standards for the management of passwords and encryption keys – they must be stored securely and encrypted, R5-117-118, R5-136-137, and user names and passwords should be unique for each user. R5-141-142. Thus, Mr. Parikh testified that Georgia's election system was grossly non-compliant with FIPS 140-2, the VVSG, and therefore with the standards for EAC certification. R-141-142. He also testified that because of the panoply of grave and unresolved security vulnerabilities, Georgia's election systems are insecure and "have no integrity." R5-82, R5-86, R5-94, R5-114.

Plaintiff's second cybersecurity expert Ben Cotton echoed these opinions based on a very impressive record of cybersecurity work for multiple federal agencies and NATO. R5-215. His work includes discovery of the Chinese hack of the Office of Personnel Management, up to that point the largest hack of U.S. Government systems ever. R5-221-222. He characterized the security of the Georgia election systems as "horrible." R5-216. He drew the following analogy:

> If I'm going to do an analogy between these vulnerabilities, you've taken an AES256 encryption key, which is a very, very

> secure encryption technology, and you've neutered it. Okay? So if I put this in an analogy with banks, if you've got a bank vault and that's the latest and greatest lock on that bank vault, and you [tout] that security on that bank vault, what they've done here is the equivalent of writing in big bold letters the combination on the wall next to the lock. Okay? So there really is no security if you can get access either remotely or physical access to those systems.

R5-267.

Mr. Cotton based his testimony upon examination of the three back-up databases produced in response to Open Records Act requests as well as upon a more detailed forensic examination of forensic images of the election systems in Coffee County, Georgia. R5-227; R5-234-235. Mr. Cotton testified that the security vulnerabilities of Georgia's election system are "appalling" R-249, and that the system is "wide open." R5-246. His examination of the Coffee County system revealed that a compiler[6] had been installed along with thousands of executable files[7] well after the install date of the certified

---

[6] Mr. Cotton explained at R5-283-284 that a compiler converts software code written by programmers into machine executable language that the computer hardware can actually interpret and execute.

[7] "An executable file is a type of computer file that runs a program when it is opened. This means it executes code or a series of instructions contained in the file." TECHTERMS.com, https://techterms.com/definition/executable_file (last visited Jan. 10, 2025).

version of the Dominion software. R5-277-278. This compiler and the thousands of executable files necessarily void any and all prior certifications. R-278-279. They are irrebuttable proof that the system that was used is not the system that was certified, which in turn is proof of the systems' lack of security and integrity.

The evidence also showed without contradiction that the Secretary has known about some or all of these vulnerabilities since no later than July 1, 2021, when an expert security analysis was delivered to his counsel in the long-running case of *Curling v. Raffensperger*, U.S. District Court, northern District of Georgia Case No. 1:17-CV-2989-AT. This 59-page report (not including exhibits) by *Curling* plaintiff's expert J. Alex Halderman, was known to or relied upon by our experts below, *see* R5-31-32, R5-86-87; R5-232, documented so many grave security vulnerabilities that U.S. District Court Judge Amy Totenberg put it under seal for nearly two years and immediately referred it to the U.S. Cybersecurity Information Security Administration ("CISA") for their review, analysis, and recommendations. R5-189-190. The Haldeman report was eventually unsealed in 2023 and released to the public in redacted form. It clearly documents the encryption

keys vulnerability by including the SQL[8] query that will retrieve them, R5-190, R5-55-56, and explaining that he was able to alter results files, encrypt them with the encryption keys and have them accepted by the system. R5-159, R5-162, just as Mr. Parikh did in his testimony in this case.

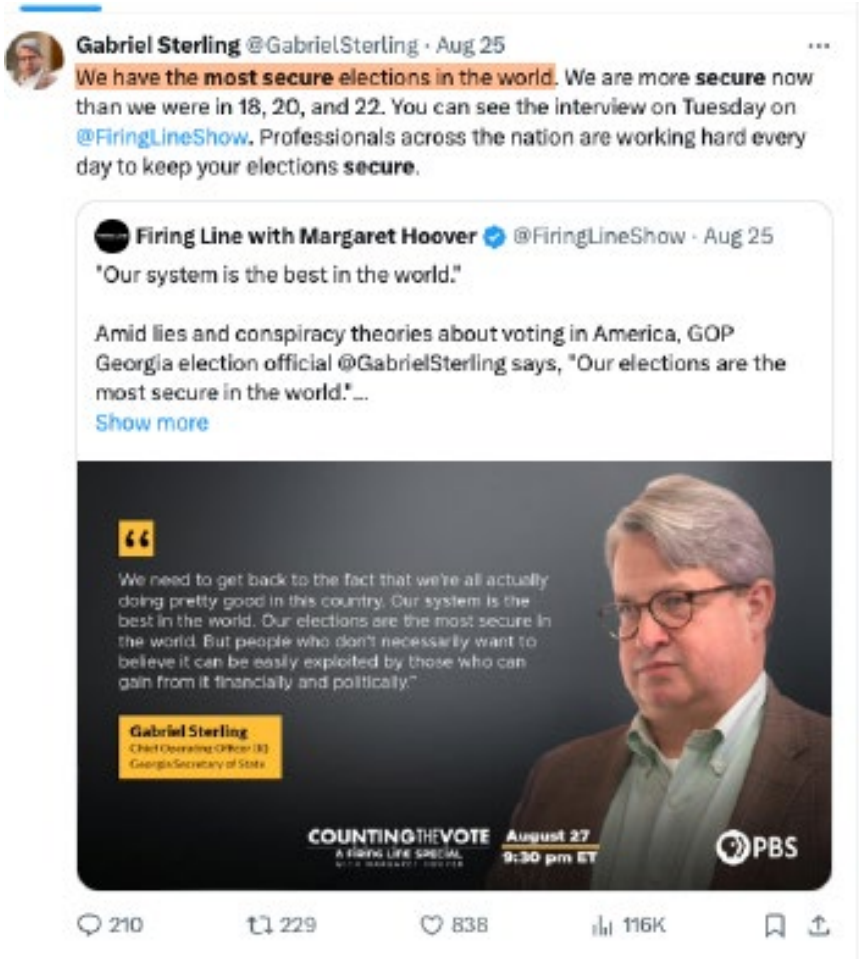
Despite knowing all these problems documented in the Halderman Report for all this time, the Secretary has done absolutely nothing to fix any of them. Whether ministerial or discretionary, the Secretary's inaction is a gross dereliction of his duties.

The evidence also showed that the Secretary of State was once again informed of the encryption keys issue and the consequent noncompliance with certification requirements in late March, 2024, when it was brought to the attention of his general counsel by Mr. Olsen, co-counsel for the Appellant. R2-11, R2-172 (the email). But the Secretary has again failed and refused to take any remedial or mitigating measures. Instead, the Secretary

---

[8] "SQL" stands for "Structured Query Language." "Structured query language (SQL) is a standardized, domain-specific programming language that excels at handling data relationships. It is used extensively for storing, manipulating and retrieving data in systems such as MySQL, SQL Server and Oracle." Tim Mucci, *What is structured query language (SQL)?,* IBM, https://www.ibm.com/think/topics/structured-query-language (last visited Jan. 10, 2025).

sent out his press flack to tell the public that the system was "the most secure in the world:"



See https://x.com/GabrielSterling/status/1827856510967332942 (last visited Jan. 14, 2025). The evidence showed this was a pluperfect lie.

The Secretary did not put on any evidence or call any witnesses.

II. Statement of Proceedings Below

The Application for a writ of mandamus was filed on August 29, 2024. R2-7. The Secretary answered and moved to dismiss on September 25, 2024,

R2-289; R2-265. The DeKalb GOP responded to the motion to dismiss on September 28, 2024 (file-stamped the following Monday, September 30). R-2-304. An evidentiary hearing was held on September 30, 2024, before the Honorable Scott McAfee of the Fulton Superior Court. *See* R5-4.

The trial court heard argument on the motion to dismiss before receiving any evidence. R5-16. The trial court reserved ruling on the motion until after hearing the Plaintiff's evidence. R5-40. After the Plaintiff's case was concluded, the State renewed its motion to dismiss and the trial court heard argument thereon. R5-287. After hearing that argument and without ruling on the motion the Court adjourned for the day and indicated that its ruling on the motion would control whether the hearing would be reconvened for the Secretary to present evidence. R5-311.

On October 3, 2024, the DeKalb GOP filed a supplemental response to the motion to dismiss. R3-137. On October 4, 2024, Judge McAfee dismissed the Application on the grounds that there was no clear legal right to mandamus relief. R4-1.

The trial court's order first rejected two arguments in the Secretary's motion to dismiss. It first held that there was insufficient evidence to support the defense of gross laches. R4-3. Secondly, it rejected the Secretary's

contention that the Plaintiff had an adequate remedy at law in the form of an election contest because it did not have standing to bring an election contest and even if it did the relief available in an election contest – limited to ordering a new election – would not remedy the violation of the law being claimed. R4-4-5.

Turning to the secretary's primary argument, the trial court agreed that mandamus relief was not available because there was no violation of any statutory duty falling on the Secretary. R4-6-7. In doing so, the trial court construed O.C.G.A. § 21-2-300(a)(2) and (3) to require no more than that the systems be certified before purchase by the Secretary and the EAC. *Id*. In other words, the trial court held that this statute imposed no duty whatsoever on the Secretary to provide systems that comply with the certification requirements during their use during elections, which is the only time it actually matters. The overwhelming and unrebutted proof that the elections systems as actually used in elections are grossly noncompliant with the cybersecurity requirements of certification was therefore legally irrelevant.

III. METHOD OF PRESERVATION OF ERROR

Error was preserved by opposing the motion to dismiss with a principal and supplemental brief, *see* R3-2 and R3-137, by twice arguing against the

motion to dismiss at the hearing, R5-16 and R5-287, and by filing a timely notice of appeal. R2-7.

SUMMARY OF ARGUMENT

O.C.G.A. § 21-2-300 imposes on the Secretary of State a legal obligation enforceable by mandamus to provide Georgia Counties with election systems that are "safe and practicable for use" and that have been certified by the EAC. The requirement of EAC certification imposed by the statute incorporates compliance with the VVSG, against which the systems are tested for purposes of certification. The VVSG further incorporates a duty to comply with FIPS 140-2. Both of these require certain minimum standards for cybersecurity and, critically, unambiguously require continuing compliance with these standards. Moreover, the Secretary's purchase contract with the election systems vendor repeatedly and emphatically requires ongoing compliance with all applicable cybersecurity standards.

The problem giving rise to this case is that in fact Georgia's election systems abjectly fail to meet these cybersecurity standards in their use in elections. The DeKalb GOP proved this with overwhelming and uncontested evidence.

The trial court, however, construed O.C.G.A. § 21-2-300 to impose only a pre-purchase certification requirement. While acknowledging that the VVSG required ongoing compliance, the trial court held the statute did not, and dismissed the case.

Proper construction of § 21-2-300(1) - (3), however, shows the trial court's analysis was erroneous. Both the plain language of the text, the statutory context in the Georgia Code and the federal Help America Vote Act, and the history of the statute and its adoption all make plain that the statutes impose a requirement on the secretary to maintain minimum standards of cybersecurity in the operational context, which is the only context in which it actually matters.

Accordingly, the Secretary breached his ministerial duties to maintain the cybersecurity of the election systems and he is subject to mandamus to compel him to perform this duty. To the extent his duties on this subject are viewed as discretionary, he has committed a gross abuse of discretion remediable in mandamus because he has known about the vulnerabilities of the system that were proved in the trial of this case since July, 2021 and has done literally nothing about other than direct his press spokesman to lie to the people of Georgia to sweep the problem under the rug.

ARGUMENT AND CITATION OF AUTHORITY

I. THE NATURE AND ELEMENTS OF MANDAMUS RELIEF.

Mandamus is an extraordinary or prerogative writ. The mandamus statutes are found at O.C.G.A. § 9-6-20 through 9-6-28. O.C.G.A. § 9-6-20 provides in relevant part that:

> All official duties should be faithfully performed, and whenever, from any cause, a defect of legal justice would ensue from a failure to perform ***or from improper performance***, the writ of mandamus may issue ***to compel a due performance*** if there is no other specific legal remedy for the legal rights; … .

(Emphasis added). O.C.G.A. § 9-6-21(a) provides that:

> Mandamus shall not lie as a private remedy between individuals to enforce private rights nor to a public officer who has an absolute discretion to act or not to act ***unless there is a gross abuse of such discretion***. However, mandamus ***shall not be confined to the enforcement of mere ministerial duties***.

(Emphasis added). The Georgia Supreme traced the doctrinal and legal history of mandamus from English common law to the present day in *Sons of Confederate Veterans v. Henry County Board of Commissioners*, 315 Ga. 39 (2022). A helpful summary of the nature and elements of mandamus relief was given in *Love v. Fulton Cnty. Bd. of Tax Assessors*:

> Mandamus is "an extraordinary remedy to compel ***a public officer*** to perform a required duty ***when there is no other adequate legal remedy***." … "The writ of mandamus is properly issued only if (1) ***no other adequate legal remedy***

> ***is available*** to effectuate the relief sought; and (2) the applicant has a ***clear legal right to such relief***." ... Further,
>
> > [f]or mandamus to issue, the law must not only authorize the act to be done, ***but must require its performance***. Where performance is required by law, a clear legal right to relief will exist either where the official or agency fails entirely to act or where, in taking such required action, the official or agency commits a gross abuse of discretion.
>
> (Citation and punctuation omitted.) ... *See also* OCGA § 9-6-21 (a) ("Mandamus shall not lie as ... to a public officer who has an absolute discretion to act or not to act unless there is a ***gross abuse of such discretion***. However, mandamus ***shall not be confined to the enforcement of mere ministerial duties***."). A gross abuse of discretion occurs where an official performs a discretionary duty ***in a manner that is arbitrary, capricious, and unreasonable***.

Love v. Fulton Cnty. Bd. of Tax Assessors, 311 Ga. 682, 692–93 (2021) (citations omitted).

Bibb Cnty. v. Monroe Cnty., 294 Ga. 730 (2014), holds that mandamus will lie to compel an official to perform an act involving the exercise of discretion but not to prescribe the outcome of the exercise. *Id.* at 738 ("While the counties therefore do have a clear legal right to a process that results in a definitive determination of the boundary line separating them, they do not have a clear legal right to any particular result of the Secretary's review process."). Mandamus "is 'the remedy for inaction of a public official.'" *Gaw v. Telfair Cnty. Bd. of Comm'rs*, 277 Ga. 157, 158 (2003) (cites omitted).

The Supreme Court in *Undercofler v. Scott* listed the categories of official conduct for which mandamus relief is available:

> The general rule is that a writ of mandamus may issue against officials to compel due performance of official duties. *Hart v. Head*, 186 Ga. 823, 199 S.E. 125; *Harmon v. James*, 200 Ga. 742, 38 S.E.2d 401. And mandamus lies against an officer to require the performance of a clear legal duty.

Undercofler v. Scott, 220 Ga. 406, 408 (1964) (citations omitted).

Of particular note, "persons holding public office may be required by mandamus to perform a continuing duty which their predecessors in office either refused or failed to do." *Id.*, *citing Weathers v. Easterling*, 153 Ga. 60 (1922) (mandamus to compel entering a contract on the minutes of the board of commissioners of roads and revenues); *Citizens' Bank of Folkston, etc. v. Newton*, 180 Ga. 860 (1935).

II. THE CYBERSECURITY REQUIREMENTS INCORPORATED INTO THE CERTIFICATION REQUIRED BY O.C.G.A. § 21-2-300(a).

As noted above, O.C.G.A. § 21-2-300(a)(3) requires any system purchased by the Secretary be certified by EAC before purchase.

EAC certification requires voting systems to be tested for compliance with the VVSG. *See* Exh. 16, R5-340 ("*Voting systems will be tested against the voluntary voting system guidelines* (VVSG), which are a set of

specifications and requirements to determine ***if the systems provide all of the basic functionality, accessibility and security capabilities required***."(Emphasis added)). Thus, to pass EAC testing for certification, a voting system must comply with the VVSG.

The Secretary admits in his answer that compliance with the VVSG is required for certification. R2-293, ¶ 114.

The VVSG specifically includes requirements for data encryption, and also adopts the Federal Information Processing Standards ("FIPS") defining the mandatory practices for protection of cryptographic keys. In particular, VVSG 1.0 (2005) requires "cryptographic keys ... use a FIPS 140-2 level 1 or higher validated cryptographic module." VVSG § 7.4.5.1(a)(i), p. 122 (Hashes and Digital Signatures); *see also id.*, § 7.5.1(b)(i), p. 125 (Maintaining Data Integrity); § 7.7.3(a)(ii), p. 132 (Protecting Transmitted Data); and § 7.9.3, p. 138 (Electronic and Paper Record Structure subsection a). The VVSG were introduced into evidence as Exh. 19, R5-358.

In short, EAC certification requires compliance with the VVSG, including its cybersecurity requirements. One of the VVSG requirements is compliance with FIPS 140-2. Therefore, through this chain, 21-2-300(a)(3)

requires compliance with FIPS 140-2, and this requires secure storage of the encryption keys.

The trial court held that while the VVSG imposed an obligation of continuing compliance, the statute did not. R4-7. This was erroneous because the statute itself necessarily incorporates compliance with EAC certification requirements which necessarily incorporate compliance with the VVSG, which unambiguously require operational compliance with the certification standards. Further, because "[a]ll statutes relating to the same subject matter are to be construed together, and harmonized wherever possible," *Hartley v. Agnes Scott College*, 295 Ga. 458, 462 (2014) (citation and punctuation omitted), this Court should also assess the Secretary's ongoing duties as part of his statutory duty to coordinate Georgia's compliance with federal law: "The Secretary of State ... shall be responsible for coordinating the obligations of the state under the federal Help America Vote Act of 2002 [HAVA]." O.C.G.A. § 21-2-50.2(a) (emphasis added). "[S]hall" denotes mandatory action, *State v. Henderson*, 263 Ga. 508, 510 (1993), and "coordinating" denotes an ongoing duty for the Secretary to abide by HAVA and its attendant VVSG standards. 52 U.S.C. § 21101(a), part of the HAVA, requires the EAC to create the VVSG to assist the states with

meeting the mandatory voting system requirements imposed by 52 U.S.C. § 21081. Compliance with the VVSG is therefore an obligation under a combination of both state and federal law that cannot be parsed out of the obligations of § 21-2-300.

III. O.C.G.A. § 21-2-300(a) Should be Construed to Require Compliance with EAC Cybersecurity Standards in the Operational Context.

In support of enumerations of error one and two, and to show the trial court erred in its reading of the certification provisions of § 21-2-300, we will start with the text, and then describe and apply the rules of construction.

1. The Text.

Below are subsections (a)(1) – (3) of O.C.G.A. § 21-2-300:

> (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 tabulated by using ballot scanners for voting at the polls and for absentee ballots cast in person, unless otherwise authorized by law; provided, however, that such electronic ballot markers 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 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***. At its own expense, the governing authority of a county may purchase, lease, or otherwise acquire additional electronic ballot markers 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 and ballot scanners by purchase, lease, or other procurement process.

2. THE RULES OF CONSTRUCTION

Georgia has both statutory and decisional law governing the construction of statutes. The codified rule at O.C.G.A. § 1-3-1(a) provides that:

> (a) In all interpretations of statutes, the courts shall look diligently for the intention of the General Assembly, keeping in view at all times the old law, the evil, and the remedy. Grammatical errors shall not vitiate a law. A transposition of words and clauses may be resorted to when a sentence or clause is without meaning as it stands.
>
> (b) In all interpretations of statutes, the ordinary signification shall be applied to all words, except words of art or words connected with a particular trade or subject matter, which shall have the signification attached to them by experts in such trade or with reference to such subject matter.

Georgia's decisional law has undergone a metamorphosis towards what is loosely referred to as "textualism." A relatively recent articulation of the decisional rules of construction was set forth in *FDIC v. Loudermilk*, 305 Ga.

558 (2019), one of many decisions construing Georgia's apportionment-of-damages statute:

> To answer that question, we first look to the text because " '[a] statute draws its meaning ... from its text.' " *Zaldivar v. Prickett*, 297 Ga. 589, 591, 774 S.E.2d 688 (2015) (*quoting Chan v. Ellis*, 296 Ga. 838, 839, 770 S.E.2d 851 (2015)). And because we "'presume that the General Assembly meant what it said and said what it meant'" when it comes to the meaning of statutes, *id.* (*quoting Deal v. Coleman*, 294 Ga. 170, 172, 751 S.E.2d 337 (2013)), "'we must read the statutory text in its most natural and reasonable way, as an ordinary speaker of the English language would.'" *Loudermilk I*, 295 Ga. at 588, 761 S.E.2d 332 (*quoting Deal*, 294 Ga. at 172-173, 751 S.E.2d 337). Important are "'[t]he common and customary usages of the words,'" which, in cases like this one, include "the usual and customary meaning of ... term[s] as used in a legal context." *Zaldivar*, 297 Ga. at 591, 596, 774 S.E.2d 688 (quoting *Chan*, 296 Ga. at 839, 770 S.E.2d 851). "For context, we may look to other provisions of the same statute, the structure and history of the whole statute, and the other law—constitutional, statutory, and common law alike—that forms the legal background of the statutory provision in question." *Id.* at 591, 774 S.E.2d 688 (citation and punctuation omitted).

Id. at 562.

Under this statement of the scope of relevant materials, the Court in *Loudermilk* considered a dizzying array of legal authorities – ranging from dictionaries, Blackstone's COMMENTARIES ON THE LAWS OF ENGLAND (1st ed. 1768), the leading treatise on torts, a lengthy catalog of Georgia cases as well as decisions from other states –to determine that the term "property" as used

in the apportionment statute, O.C.G.A. § 51-12-33, included intangible property. *See Loudermilk*, 305 Ga. at 562-68. *Loudermilk* demonstrates that the Georgia decisional rules of statutory interpretation are not a straitjacket as some would have it — a court may and where necessary should look far and wide to make sense of statutory language. There is no compulsion to absurdity.

Whether the tenets of Georgia's textualism are in tension with the statutory directive of O.C.G.A. § 1-3-1(a) that statutes should be construed "keeping in view at all times the old law, the evil, and the remedy" is a question that has arisen from time to time.[9] However, the tension is likely illusory because the flexibility in the contextual textualism of cases like *Loudermilk* embraces the "purposivism" of § 1-3-1(a), or at least blurs to the point of erasure the notional distinctions between purposivism and textualism. The apparent tension between purposivism and textualism is more a function of how commentators define these terms as a matter of

[9] For an example of the seeming tension, compare the majority and dissenting opinions *Patton v. Vanderpool*, 302 Ga. 253 (2017) and *Bellsouth Telecommunications, LLC v. Cobb County*, 342 Ga. App. 323, 335 n. 3 (2017) (Dillard, P. J., concurring) *reversed*, *Bellsouth Telecommunications, LLC v. Cobb Cnty.*, 305 Ga. 144 (2019).

theory than how courts apply them in practice. There is sufficient free play in how Georgia courts apply textualism that textualism largely overlaps with purposivism, dissolving the perceived tension. *See, e.g*. John F. Manning, *The New Purposivism*, 2011 SUP. CT. REV. 113 (noting adoption of textualist precepts by purposivist judges); Jonathan T. Molot, *The Rise and Fall of Textualism*, 106 COLUM. L. REV. 1, 2–3 (2006) (noting convergence of textualism and purposivism in consideration of contextual factors); Charles M. Cork, III, *Reading Law in Georgia*, (available at https://tinyurl.com/4c92jhrr (last visited Jan 14, 2024) (vigorously critiquing Justice Antonin Scalia and Brian Garner's READING LAW, and tracing history of Georgia's blended approach from the earliest cases to the date of publication). And, in any case, strict textualism would require the purposivist terms of O.C.G.A. § 1-3-1(a) be given effect according to their plain meaning.

If the distinction between textualism and purposivism is much ado about not very much, this flexibility portends fewer aberrant results from extreme or arid textualism.[10]

---

[10] An example of arid textualism leading to an absurd and erroneous result is *Giller v. Slosberg*, 359 Ga. App. 867 (2021), which was reversed by a

3. APPLICATION OF THE RULES OF CONSTRUCTION

a. Textual analysis.

The phrase in subsection § 21-2-300(a)(2) requiring the Secretary to certify that the system is "***safe and practicable for use***" on its face refers to the actual use of the system. Under the trial court's interpretation, this certification requirement applies not to the use of the system but only to its pre-purchase testing. But using and testing a system are clearly distinct concepts in their definitions and commonly understood meanings.

The Oxford Language online dictionary at Google and the Merriam-Webster Online dictionaries give the following meanings of "use" and "test:"

	OXFORD LANGUAGE	MERRIAM-WEBSTER
"Use"	(noun) "the action of using something or the state of being used for a purpose." (verb) "take, hold, or deploy (something) as a means of accomplishing or achieving something; employ."	(noun) "the act or practice of employing something (verb) "to put into action or service; avail oneself of"

broader contextual and purposivist approach in *Slosberg v. Giller*, 314 Ga. 89 (2022).

"Test"	(noun) a procedure intended to establish the quality, performance, or reliability of something, especially before it is taken into widespread use. (verb) Take measures to check the quality, performance, or reliability of (something), especially before putting it into widespread use or practice.""	(noun) "a critical examination, observation, or evaluation." (verb) "to put to test or proof"

b. Legal Context

In *Loudermilk*, the Court held that "For context, we may look to other provisions of the same statute, the structure and history of the whole statute, and the other law—constitutional, statutory, and common law alike—that forms the legal background of the statutory provision in question." 305 Ga. At 562 (interior quotation marks omitted).

Other provisions of the same statute are thus properly considered and they too illustrate the trial court's error. The immediately preceding subsection, (a)(1), tells us unambiguously that the systems under discussion are for "use" in elections: "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." In (a)(2) "such systems' must be certified by the Secretary of State.

The point is again illustrated by the first sentence of subsection § 21-2-300(a)(3), especially when read along with (a)(1) and (a)(2): "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." (Emphasis added). In (a)(3) "such equipment" being certified refers to the equipment that will be "used." It is clear and unambiguous from these provisions when read together as they should be that the legislature is requiring the machines ***that will be used*** in the operational context in elections be safe, reliable and compliant with the EAC certification requirements, and that certification by the Secretary and the EAC is the chosen means to achieve that end,. The obvious and reasonable expectation was that a system certified as compliant before purchase will actually be compliant in use. Holding otherwise ascribes to the legislature a nonsensical intent to forfeit the benefit of the bargain – compliance with the certification standards.

c. EAC testing program documents require ongoing compliance with certification standards.

Because the statute requires EAC certification, the legal context for construing the statute necessarily also includes the terms and conditions of EAC certification testing generally and with respect to cybersecurity particularly.

As one would expect, documents from the EAC support the conclusion dictated by common sense: systems must comply with certification requirements in the operational environment of the systems' use in elections.[11]

EAC's website explains:

> The purpose of the EAC's national voluntary voting system certification program is to independently verify that voting systems comply with the functional capabilities, accessibility, and security requirements necessary to ensure the ***integrity and reliability of voting system operation,*** as established in the Voluntary Voting System Guidelines (VVSG).

EAC Testing and Certification Program, EAC, August 11, 2021, available at https://www.eac.gov/sites/default/files/TestingCertification/EAC_Testing_and_Certification_Program.pdf, (last visited Jan 14, 2025) (emphasis

[11] The materials cited in this section were briefed to the trial court in the DeKalb GOP's Supplemental Response to the Motion to Dismiss. R3-137.

added).

This document further explains that "the VVSG ***covers pre-voting, voting, and post-voting operations***." *Id*. p. 6 (emphasis added).

Under the heading "Security," the document states:

> - System integrity requires risk assessment and supply chain risk management strategy, removes non-essential services, ***requires exploit mitigation*** … and ***the system to be free of known vulnerabilities***, cryptographic boot validation, and authenticated updates.
>
> - ***Data protection requires FIPS 140-2 validated cryptographic modules*** (except E2E), cryptographic protection of various election artifacts and digitally signed cast vote records and ballot images.

Id. at p. 7. Regarding post-certification operational compliance, EAC explains its Quality Monitoring Program as follows:

> After a system is certified, the manufacturer assumes primary responsibility for compliance of the products produced. … . ***These additional tools help ensure that voting systems continue to meet the VVSG requirements as the systems are manufactured, delivered, and used in federal elections.*** These aspects of the program enable the EAC to independently monitor the continued compliance of fielded voting systems.

Id. at p. 12 (emphasis added).

> The purpose of the Quality Monitoring Program is to:
>
> • Ensure systems used by election jurisdictions are identical to those tested and certified by the EAC.

• Monitor the completeness and adequacy of testing ***with the desired performance in fielded voting systems***.

• Monitor the effectiveness of the VVSG.

Id. (Emphasis added).

The EAC's own descriptions of its testing and certification program ratify the obvious common-sense plain language meaning of the statute that compliance in the operational environment is required, and thus refute the trial court's key conclusion that there is no requirement to comply with certifications standards while the machines are being used in elections.

d. <u>FIPS 140-2 requires operational compliance.</u>

FIPS 140-2, Applicant's Exhibit 20 at R5-582, is also incorporated as a legal requirement for Georgia's elections system, *Curling v. Raffensperger*, 493 F. Supp. 3d 1264, 1290 n.51 (N.D. Ga. 2020) (quoted *infra*), and also` ***unambiguously*** requires operational compliance. The term "operational environment" appears 28 times in the document and is the title of Section 4.6 of the document. FR5-588, 616. Security requirements are defined to apply to the operational environment, with the requisite measures escalating according to the specified security level.

e. Modifications to ensure continuing compliance are managed through engineering change orders.

In further proof that compliance with the standards for EAC certification is an ongoing requirement, the EAC requires submitting an Engineering Change Order ("ECO") for EAC's review and approval when vendors make a change to their systems:

> Any proposed change that is not deemed to be a minimal change is a modification and must be submitted for testing and review consistent with the EAC Testing and Certification Program requirements.

Engineering Change Orders, U.S. ELECTION ASSISTANCE COMMISSION, January 24, 2024, available at https://www.eac.gov/voting-equipment/engineering-change-orders (last visited Jan. 14, 2025). Dominion's ECOs will be retrieved for display by this link: https://www.eac.gov/voting-equipment/engineering-change-orders?f%5B0%5D=manufacturer%3A56081 *Id.* (last visited Jan. 14, 2025).

f. The Secretary's contract with the system vendor requires operational compliance.

The contract between the State and the election system vendor, attached to the Application as Exh. 1, R2-39, requires that the systems "***meet all Mandatory Requirements***" and "***accurately function in accordance with those requirements... enabling State and all***

other State Entities to accurately and securely administer elections throughout the State of Georgia in accordance with Applicable Laws of the State of Georgia." Contract at § 1.2 (emphasis added). This incorporates the certification requirements in O.C.G.A. § 21-2-300 and unambiguously requires the systems be compliant with those requirements during their use in elections. In the Contract, the vendor also represents that "proper system and software hardening procedures are clearly defined and regularly tested. Data integrity and confidentiality is also implemented according to NIST defined and FIPS validate [sic] procedures and algorithms." *Id.*, Exh. B to Contract, § 8.9. "Dominion implements security protocols that meet or exceed EAC VVSG 2005 requirements. All of Dominion's security protocols are designed ***and implemented to stay current*** with the rapidly evolving EAC security requirements set forth by various iterations of the VVSG." Exh. B to Contract, section 8. "Data generated by the Democracy Suite platform is protected by the deployment of FIPS-approved symmetric AES and asymmetric RSA encryption." (*Id.*, section 8.3).

On the topic of cybersecurity, the Contract requires the vendor to carry out periodic security assessments and give timely notice of any security breaches:

> § 7 Compliance
>
> > § 7.2.1 … Contractor, at its own expense, will undertake such actions, and implement such changes, as reasonably necessary to remedy any material deficiencies, concerns or recommendations identified through any audits, examinations, or tests described in this Section 7.2.1 and ***ensure Contractor's continued compliance with Contractor's obligations as relate data security under this Agreement.***
> >
> > 7.2.2 Contractor further agrees that it shall: …
> >
> > (b) Notify the State Entity's primary security contact of an actual or security breach or the suspicion of the occurrence of a security breach (hereinafter a "Breach Incident") as soon as practical but no later than forty-eight hours after Contractor becomes aware of a Breach Incident ….

Contract § 7, p. 13.

When the Secretary decided to buy the current election systems, his contract required with exceptional clarity and vigor that the systems comply with certification requirements while being used during elections. He now says in Court there is no such requirement. He cannot have it both ways.

g. A Predecessor Secretary of State contended that insecure encryption keys were a serious security issue.

In the trial court, one of the *amici* (Cherokee County Republican Party, et al), pointed out that in *Smith v. DeKalb Cnty.*, 288 Ga. App. 574, 577 (2007), former Secretary of State Cathy Cox sought and obtained an injunction to block a county's production in response to an Open Records Act of certain sensitive election records. R3-44, 49-50. The request was for election information that would include the election system's encryption keys. The Secretary's position in that case was that "release of the CD-ROM, which contains passwords, encryption codes, and other security information, ***would compromise election security***." 288 Ga. App. at 577. (Emphasis added). The ruling was also based on the testimony of "Smith's witness ... that he could break the encryption codes with software from other sources." *Id*. The previous Secretary recognized that security of encryption keys is an elementary requirement of election security. Indeed, the current Secretary also recognized the same thing when he negotiated the terms of the contract with Dominion.

Yet the current Secretary now takes a conflicting position, arguing that the encryption keys issue is merely hypothetical and that any risks are sufficiently mitigated by other security measures such as physical security.

The Secretary should not be heard to so cavalierly contradict both himself and his predecessor on such a serious issue. FIPS 140-2, the VVSG, EAC certification and O.C.G.A. § 21-2-300 all require secure storage and management of encryption keys in the operational environment. The Secretary's position reeks of mendacity and should not be tolerated.

The Secretary is not entitled to pick and choose which parts of the certification requirements he will obey. It is an all-or-nothing proposition. In *Curling v. Raffensperger*, the evidence showed that the Secretary and Dominion rushed to install a last-minute software update to fix a bug just before the 2020 election. The bug fix was not EAC-certified and thus the installation violated the certification requirements ***in the operational context***. The court dispatched the Secretary's half a loaf argument as follows:

> While state participation in EAC's review and approval regime is voluntary, once a state has elected to do so as in Georgia's case, the EAC treats state compliance with its standards and procedures as required. ***There is no provision for half compliance or half participation in EAC's review procedures.***

Curling, 493 F.Supp.3d at 1290, n.51. (Emphasis added). The court in *Curling* quite obviously recognized that compliance with the certification requirements extended to the use of the systems in elections. The Secretary's

position here that certification is a one-and-done pre-purchase affair is contrary to law.

4. HISTORY LEADING TO ADOPTION OF O.C.G.A. § 21-2-300.

At the hearing, counsel for the Secretary directed the trial court to an article describing the legislative history of the legislation. *See* Beth K. Boatright and Andrew Smith, *HB 316 - Voting System*, 36 GEORGIA STATE U. L. REV. 81, 85 (2019). While what has been said already is sufficient to show the trial court's error, the article supports the DeKalb GOP's position because it explains that cybersecurity was "at the forefront of both legislative and judicial attention" as a result of not only reports of Russian attempts to hack the 2016 election but also pressure from Judge Totenberg in the *Curling* litigation that she was on the verge of ordering the State replace the Diebold DRE system, which in fact she did.

Part of that history was the formation of the Secure, Accessible & Fair Elections (SAFE) Commission to make recommendations to the legislature on a replacement voting system. Both the acronym, "SAFE," and its first

word, "Secure," reflect the importance of cybersecurity in the process.[12] One of the principal reasons for creating the Commission was to address concerns about cybersecurity on the existing system. *Id.* p. 1. Recommendation #5 called for adherence to best cybersecurity practices.

Secretary Raffensperger emphasized in his remarks to the Commission said that "the priceless franchise to vote requires free, clean and accurate elections throughout every aspect of the election process," and that "we need the most secure, updated voting technology." Transcript of Proceedings before the SAFE Commission, December 12, 2018, https://sos.ga.gov/sites/default/files/2022-03/safecommissiontranscript12.12_.18_.pdf (last visited Jan. 14, 2025).

All the factors described above, along with this legislative history together satisfy the necessary elements to apply the mischief rule codified in O.C.G.A. § 1-3-1(a), directing that "courts shall look diligently for the intention of the General Assembly, keeping in view at all times the old law, the evil, and the remedy." By not imposing any cybersecurity requirements,

[12] The Commission's report is found at https://sos.ga.gov/sites/default/files/2022-03/safe_commission_report_final_1-10-18.pdf (last visited Jan. 13, 2025).

the old law permitted the use of an insecure system. The evil is the risk of hacking an election, a prominent concern driving the adoption of § 21-2-300 in the wake of the 2016 presidential election, as many Democrats believe to this day that the Russians hacked the election in favor of President Trump. The remedy to this evil was to require that the machines meet the standards of EAC certification, including the cybersecurity requirements, which themselves unambiguously and emphatically require compliance during elections. Compliance during elections is the point of the whole exercise. Moreover, the legislature added a general requirement that the Secretary provide a second certification that the systems are "safe and practicable for use."

Properly construed, O.C.G.A. § 21-2-300(a)(1) – (3) require the Secretary to field election systems that comply with the requirements of certification during their use in elections. The trial court erred in holding to the contrary and should be reversed.

IV. THE SECRETARY HAS BREACHED HIS DUTY TO ENSURE THAT GEORGIA'S ELECTION SYSTEMS COMPLY WITH THE APPLICABLE CERTIFICATION REQUIREMENTS.

Construing the statute as discussed above, the Secretary has a ministerial duty to ensure that the election systems he requires the counties

to use comply with the EAC certification standards during their use in elections. The 2024 election is over, but another election will come along soon enough. The Secretary's duty should be enforced by mandamus.

Even if the Secretary's duty is viewed as discretionary, he is subject to mandamus because of the clear abuse of that discretion. The Secretary has statutory discretion to revisit the ongoing safety of election equipment, O.C.G.A. § 21-2-324(a). And he has no discretion to certify or require a system that is proven by overwhelming and uncontested evidence to be not "safe and practicable for use" and which does not meet the requirements for EAC certification. The Secretary does not have discretion to ignore the fact that the encryption keys are left in plain text and unprotected from unauthorized use, in violation of express EAC certification requirements and directly contrary to his own certification and rendering any election open to undetectable compromised.

Despite being on notice of the unprotected encryption keys issue since July of 2021, the Secretary has taken no action. Even if his duties are discretionary, which they are not, the contours of the Secretary's discretion cannot shelter ignoring such an urgent cybersecurity threat for such a long time and directing his press spokesman to deceive the public with ridiculous

lies. That is a clear and compelling abuse of discretion for which mandamus relief will lie.

CONCLUSION

O.C.G.A. § 21-2-300 does not permit the Secretary to field election systems that are abysmally noncompliant with the EAC certification standards for cybersecurity. Nor does it allow him totally ignore the problem for years after it was brought to his attention. His duty is continuing, and should be enforced by mandamus. The trial court's dismissal should be reversed and the Secretary should be ordered to fix the appalling and egregious security weaknesses he has ignored for more than three years.

Respectfully submitted, this January 15, 2025.

This submission does not exceed the word count limit imposed by Court of Appeals Rule 24.

CALDWELL, CARLSON, ELLIOTT & DELOACH, LLP

/s/ Harry W. MacDougald
Harry W. MacDougald
Ga. Bar No. 463076
6 Concourse Parkway
Suite 2400
Atlanta, Georgia 30328
(404) 843-1956
hmacdougald@ccedlaw.com

HARDING LAW FIRM, LLC

/s/ Todd A. Harding
Todd A. Harding, For the Firm
Ga. Bar No.: 101562
Attorney at Law
HARDING LAW FIRM, LLC
113 E. Solomon Street
Griffin, Georgia 30223
(770) 229-4578
(770) 228-9111 facsimile

CERTIFICATE OF SERVICE

Consistent with Court Rule 6(b)(2), I certify that there is a prior agreement with the below-listed counsel for the Appellee to allow documents in a PDF format sent via email to suffice for service, and that contemporaneously with filing a copy of this filing was emailed to them at the email addresses indicated below:

Elizabeth T. Young, Esq.
Alexandra Noonan, Esq.
Office of the Attorney General
Chris Carr
40 Capitol Square SW
Atlanta Georgia 30334
eyoung@law.ga.gov

Charlene S. McGowan, Esq.
General Counsel to the Secretary of State of the State of Georgia
214 State Capitol SW
Atlanta GA 30334-1600
cmcgowan@sos.ga.gov

Bryan P. Tyson, Esq.
Taylor English Duma LLP
1600 Parkwood Circle Suite 200
Atlanta GA 30339
btyson@taylorenglish.com

This January 15, 2025.

CALDWELL, CARLSON, ELLIOTT & DELOACH, LLP

/s/ Harry W. MacDougald
Harry W. MacDougald

Ga. Bar No. 463076
6 Concourse Parkway
Suite 2400
Atlanta, Georgia 30328
(404) 843-1956

hmacdougald@ccedlaw.com