IN THE SUPERIOR COURT OF FULTON COUNTY

STATE OF GEORGIA

DEKALB COUNTY REPUBLICAN PARTY, INC. APPLICANT, V. BRAD RAFFENSPERGER, IN HIS OFFICIAL CAPACITY AS THE SECRETARY OF STATE OF THE STATE OF GEORGIA, RESPONDENT	Civil Action File No. 24CV011028

APPLICANT'S RESPONSE TO MOTION TO DISMISS

CALDWELL, CARLSON, ELLIOTT & DELOACH, LLP

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

Todd A. Harding, For the Firm
Ga. Bar No.: 101562
113 E. Solomon Street
Griffin, Georgia 30223
(770) 229-4578
(770) 228-9111 facsimile

OLSEN LAW, P.C.

Kurt B. Olsen*
1250 Connecticut Ave., NW, Ste. 700
Washington DC 20036
(202) 408-7025
ko@olsenlawpc.com

** Pro Hac Vice Application pending*

TABLE OF CONTENTS

COMES NOW, the DeKalb County Republican Party, Inc. ("DeKalb GOP"), and submits this brief in response to the motion to dismiss of the Secretary of State (the "Secretary").

INTRODUCTION

The Secretary seeks dismissal on various grounds which upon examination are without merit and should be rejected. First, he contends that the Applicant has no clear right to relief because the Dominion system used in Georgia was in fact certified by the Election Assistance Commission ("EAC") prior to purchase. Second, the Secretary contends that mandamus relief is barred because the Applicant has an adequate remedy at law in the form of an election contest. Third, he contends the relief sought is not available in a mandamus case. Finally, he argues that the claim is barred by laches.

As will be shown below, these arguments are without merit and the motion should be denied.

I. THE NATURE AND ELEMENTS OF MANDAMUS RELIEF.

Mandamus falls into the category of the extraordinary or prerogative writs. The relevant 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).

The Georgia Supreme traced the doctrinal and legal history of mandamus from English common law to today in *Sons of Confederate Veterans v. Henry County Board of Commissioners*, 315 Ga. 39 (2022) ("*SCV*"). The case of *Love v. Fulton Cnty. Bd. of Tax Assessors* gives a useful summary of the nature and elements of mandamus relief:

> Mandamus is "an extraordinary remedy to compel ***a public officer*** to perform a required duty ***when there is no other adequate legal remedy***." (Citation and punctuation omitted.) *R. A. F. v. Robinson*, 286 Ga. 644, 646 (1), 690 S.E.2d 372 (2010). "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***." (Citation and punctuation omitted.) *Ga. Assn. of Professional Process Servers v. Jackson*, 302 Ga. 309, 312 (2), 806 S.E.2d 550 (2017). 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.) *Id*. at 312-313 (2), 806 S.E.2d 550. 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***. *See Massey v. Georgia Board of Pardons & Paroles*, 275 Ga. 127, 128 (2), 562 S.E.2d 172 (2002).

Love v. Fulton Cnty. Bd. of Tax Assessors, 311 Ga. at 692–93.

In this case, the DeKalb GOP seeks enforcement of the Secretary's ministerial duty to comply with O.C.G.A. § 21-2-300 and the incorporated requirements that the

election system in Georgia meet the requirements of certification by the EAC, which in turn mandates compliance with the Voluntary Voting Systems Guidelines (VVSG) and the Federal Information Protection Standards (FIPS 140-2). The Application alleges and the evidence will show that the election system fielded by the Secretary utterly fails to comply with these vital security requirements with respect to the storage of encryption keys, a serious breach of cyber security requirements of the certification standards. The Secretary has no discretion to field and require use of election systems that fail to meet these requirements.

II. THE APPLICANT HAS A CLEAR LEGAL RIGHT TO THE REQUESTED RELIEF.

The Secretary's first group of arguments are offered to make the overriding point that the DeKalb GOP has no clear legal right to mandamus relief. The Secretary contends that he has already fully complied with all legal requirements pertaining to certification, that his certification that the election systems are "safe and practicable for use" is not subject to challenge by mandamus, and that he is not a proper party for mandamus relief with respect to a regulation of the State Election Board. These arguments rely on mischaracterizations of the law and of the Applicant's arguments and should be rejected. We first review our allegations of noncompliance with the certification requirements and then address the Secretary's arguments.

1. THE SECRETARY HAS BREACHED A MINISTERIAL LEGAL DUTY TO ENSURE THAT ENCRYPTION KEYS ARE STORED AS REQUIRED BY THE APPLICABLE CERTIFICATION REQUIREMENTS.

As set forth in the Application, the Secretary is responsible for fielding a uniform election system in Georgia. O.C.G.A. § 21-2-300(a)(1) provides: "(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." The Secretary must certify the equipment as "*safe and practicable for use*." O.C.G.A. § 21-2-300(a)(2) (emphasis added).

O.C.G.A. § 21-2-300(a)(3) provides that "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).

As plead in the Application EAC certification requires voting systems to be tested for compliance with the VVSG. *See* U.S. Election Assistance Commission, Certified Voting Systems, https://www.eac.gov/voting-equipment/certified-voting-systems (last visited Sept. 27, 2024) ("*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 that compliance with the VVSG is required for certification. MTD, pp. 6-7.

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). VVSG 1.0 (2005) is available here: https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.0_Volume_1.PDF (last visited Sept. 27, 2024).

The Application alleges, supported by testimony from Applicant's expert witnesses in affidavits attached to the Application and to be presented at trial, that the election systems fielded by the Secretary do not comply with these requirements in that the encryption keys are stored unprotected and in plain text in the election database and can be retrieved with a straightforward SQL query by anyone, whether an insider or outsider, who can get past the Windows log-in, which in cybersecurity circles is a trivial obstacle. The Application alleges that the system falls woefully short of the secure storage of encryption keys required by the combination of (1) O.C.G.A. § 21-2-300(a)(3)

(requiring EAC certification); (2) EAC certification (requiring compliance with VVSG); (3) the VVSG (requiring compliance with FIPS 140-2); and (4) FIPS 140-2 (requiring secure storage of encryption keys). Moreover, this vulnerability fails the requirement that Georgia's election systems be "safe and practicable for use." § 21-2-300(a)(2).

The Application further alleges that it is not just Applicant's experts who have noted the insecure storage of the encryption keys and the gravity of the threat is poses to election security. As noted above, in the *Curling* litigation, Plaintiff's expert Professor Halderman prepared a sealed expert report dated July 1, 2021 (later unsealed) that was delivered to the Secretary's attorneys at that time, that noted the encryption keys were stored in plain text in the election database and could be retrieved with a SQL query that he included in his report in Section 9.1.

On a motion to dismiss, these allegations must be taken as true. *Greene County School Dist. v. Circle Y Constr., Inc.*, 291 Ga. 111, 112,(2012). (The appellate court "review[s] de novo the trial court's ruling on the [defendants'] motion to dismiss, accepting as true all well-pled material allegations in the complaint and resolving any doubts in favor of [the plaintiff]."); *Williams v. DeKalb Cnty.*, 308 Ga. 265, 267 (2020).

2. COMPLIANCE WITH CERTIFICATION REQUIREMENTS IS AN ONGOING DUTY THE SECRETARY HAS BREACHED.

The Secretary argues in his motion that in fact the Dominion system in Georgia is certified by the EAC and that he certified the system as "safe and practicable for use, and that nothing more is required by O.C.G.A. § 21-2-300(a)(3). *See* MTD, pp. 11-12. The

Secretary explicitly contends that there is no ongoing obligation that the operational system comply with the certification requirements. MTD at pp. 12-13. According to this argument, even definitive proof that the system does not actually comply with the certification requirements and is not in fact "safe and practicable for use" simply does not matter and does not constitute a violation of Georgia law remediable by mandamus.

This argument elevates the pre-purchase EAC certification into an irrebuttable presumption of compliance ever after. But the true meaning of a certification is that the system was compliant at the time of inspection. It does not and cannot preclude future noncompliance. To create the conclusive, irrebuttable presumption implicit in the Secretary's argument would require a clear statement from the legislature, which does not exist.

A further problem with the Secretary's argument is the contention that his obligations under Georgia law relating to certification and cyber security cease to exist upon certification – which occurs prior to purchase – and do not extend to the actual operation of the systems during elections. This makes no sense.

First and foremost, it is precluded by the requirement that the Secretary himself certify the system as "safe and practicable ***for use***" O.C.G.A. § 21-2-300(a)(2). The certification on its face relates to the safety of the systems in operational environment during elections.

The Secretary's argument to the contrary renders the certification requirement an empty gesture and nullifies the obviously intended substantive requirements that the system meet cyber security standards so that it can be safely used in elections and not merely in a testing lab. The Secretary's argument cannot be reconciled with the plain language of the VVSG, which requires ongoing compliance, including correction of any deficiencies that become known. Thus, the VVSG imposes a requirement of "quality assurance":

> Quality assurance provides ***continuous confirmation that a voting system conforms with the Guidelines*** and to the requirements of state and local jurisdictions. Quality assurance is a vendor function that is initiated prior to system development ***and continues throughout the maintenance life cycle of the voting system***."

Section 8.1, p. 147 (emphasis added). *See also* § 9.5(d) (discussing establishment of procedures to resolve identified defects).

The Contract between the State and Dominion similarly requires that the system *"**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). The Dominion Contract also represents that "In addition, 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 procedures and

algorithms" *Id*., Exh. B to Contract, § 8.9. The Contract further provides that "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. Further, the Contract requires that "[d]ata generated by the Democracy Suite platform is protected by the deployment of FIPS-approved symmetric AES and asymmetric RSA encryption." (*Id*., section 8.3).

The provisions show beyond dispute that the Secretary bargained for ***operational compliance*** with applicable certification requirements. Yet he now argues there is no such obligation. Which is it, Mr. Secretary?

The Secretary's argument offends basic principles of statutory construction because it would render the certification requirement a mere formality in purchasing, and a nullity in the operational environment where it is clearly intended to have meaning. "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." O.C.G.A. § 1-3-1(a). The evil is an election system unprotected from cyber threats, and the remedy is a system that complies with the cyber security certification requirements. The rules of statutory interpretation steer courts away from interpretations that would render statutes absurd, futile or a nullity:

> "It is the duty of the court to consider the results and consequences of any proposed construction and not [to] so construe a statute as will result in

> unreasonable or absurd consequences not contemplated by the legislature." (Citations, punctuation and emphasis omitted.) *Gen. Elec. Credit Corp. c. v. Brooks*, 242 Ga. 109, 112 (249 SE2d 596) (1978). "In the construction of [any] statute a court may decline to give a legislative act such construction as will attribute to the General Assembly an intention to pass an act which is not reasonable, or as will defeat the purpose of the proposed legislation." (Citation and punctuation omitted.) *Bd. of Trustees of the Policemen's Pension Fund v. Christy*, 246 Ga. 553, 554 (1) (272 SE2d 288) (1980). In construing statutes, interpretations which cause an unreasonable intent to be found, an intent to do an unreasonable thing, or intent to do futile and useless things, will not be found to be the legislative intent; instead, the construction of intent should further the purpose of the Act. *Trust Co. Bank v. Ga. Superior Court Clerks' Coop. Auth.*, 265 Ga. 390 (456 SE2d 571) (1995); *City of Jesup v. Bennett*, 226 Ga. 606, 609 (176 SE2d 81) (1970).

Lamad Ministries v. Board of Tax Assessors, 268 Ga. App. 798, 802 (2004). *See also Haugen v. Henry County*, 277 Ga. 743(2) (2004) ("The judiciary has the duty to reject a construction of a statute which will result in unreasonable consequences or absurd results not contemplated by the legislature.")

The Secretary's position that he has no duty to ensure compliance with the requirements of certification during elections reduces certification to no more than security theatre. It defies common sense to argue that a requirement that a system be certified as secure does not also require that it actually be secure in ongoing operation, but that is precisely the argument the Secretary is making.

The Applicant has a clear legal right under O.C.G.A. § 21-2-300 to an election system that in its operation meets the requirements of EAC certification. The Secretary is at pains to reassure the public that election systems are safe and secure *during*

elections. The Application alleges and the evidence filed with it shows the system does not meet those requirements, the EAC certification notwithstanding.

To support the argument that the Applicant has no clear legal right to mandamus relief, the Secretary attempts to recharacterize the relief that is actually sought into relief not actually sought that is easier to defend – the classic straw man fallacy. The Applicant seeks an order compelling the Secretary to perform his duty to field a system compliant with certification requirements, while the Secretary repeatedly recharacterizes the relief sought as an order that the Secretary "second guess the prudence of the EAC's certification" or "override the determination of a federal agency," MTD at 3, or "Applicant cannot use mandamus to compel the Secretary to investigate the EAC's certification methodology or compliance decisions, nor does he have the legal authority to oversee the determinations of a federal agency." *Id*. at 9. These are straw man arguments because no such relief is sought. Instead, the Application seeks enforcement of the Secretary's independent, ministerial, non-delegable duties under State law to field a system that meets the applicable requirements in ongoing operation. No allegation of breach of duty by the EAC is made, though we certainly do not rule it out. The allegation here is that the Secretary breached *his* duties under *state* law and the remedy sought is for that breach.

For the sake of argument, we could assume the EAC correctly certified the system on January 19, 2019. While this pre-purchase certification would be some

evidence that the systems was compliant at that time, it at most supports only an inference of compliance at present. The allegation, supported by competent expert testimony, is that the system is noncompliant *now*, and this must be taken as true for purposes of the motion to dismiss.

3. THE SECRETARY'S BREACHES OF HIS LEGAL DUTIES ARE REMEDIABLE BY A WRIT OF MANDAMUS.

Building on these mischaracterizations of the relief sought and the claim that there is no ongoing duty of compliance, the Secretary contends that mandamus cannot be used to challenge his previous certification that the system is "safe and practicable for use," because mandamus can only compel the performance of an act, and not the manner of its performance. MTD at 13-14. The answer to this argument is O.C.G.A. § 9-6-20, which provides 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). The emphasized language clearly authorizes relief from "improper performance," and clearly authorizes the compulsion of a "due performance."

The Secretary also argues that his determination is discretionary and that mandamus cannot compel the performance of a discretionary act. But O.C.G.A. § 9-6-21 clearly states that mandamus relief "shall not be confined to the enforcement of mere ministerial duties." The cases quoted by the Secretary, as well as those quoted by the

Applicant above, provide that mandamus will lie where there has been a gross abuse of discretion. MTD at pp. 8, 10, 13. The Application alleges a gross abuse of discretion at paragraph 36 in fielding and leaving in place a system that is egregiously noncompliant with the cybersecurity requirements of certification, particularly after receiving notice of the encryption keys vulnerability in July 2021.

III. AN ELECTION CONTEST IS NOT AN ADEQUATE LEGAL REMEDY.

The Secretary contends in division II of his brief (p. 16) that the Applicant has an adequate remedy at law in the form of an election contest under O.C.G.A. § 21-2-520 et seq. Though it is true that an adequate remedy at law is a defense to mandamus, *Love v. Fulton Cnty. Bd. of Tax Assessors, supra,* this argument is groundless and utterly without merit.

First, the DeKalb GOP cannot pursue an election contest remedy because O.C.G.A. § 21-2-521 grants the right to bring such a claim to "any person who was a candidate at such primary or election for such nomination or office, or by any aggrieved elector who was entitled to vote for such person or for or against such question." The DeKalb GOP cannot be either a candidate or an aggrieved elector and so has no standing to bring an election contest, period.

Second, even if it did, the relief sought here is simply not available in an election contest, which is limited to declaring the contested election invalid and ordering a new election. *See* O.C.G.A. § 21-2-52(b). There is no provision in the election contest statute

for enforcing the Secretary's duty to field a system that complies with the cybersecurity requirements of certification.

Third, and again assuming the DeKalb GOP could bring an election contest (which it cannot), and that it could seek enforcement of the Secretary's duty to field a compliant system (which it cannot), there would be likely insuperable difficulty in proving that any exploit of the encryption keys vulnerability was sufficient to place the outcome in doubt as required for an election contest alleging an irregularity in the vote. *See* Application for Mandamus, ¶s 46-50; O.C.G.A. § 21-2-522(1), (3), (4) and (5). The testimony from Applicant's expert witnesses in affidavits attached to the Application and in their testimony to be presented at trial shows that the nature of the encryption keys makes it extremely difficult to detect an exploit after the fact.

The Secretary argues that Applicant seeks relief for a purely hypothetical problem and does not allege any prior exploitation of the encryption keys vulnerability. This argument is deeply flawed for at least two reasons. First, no such allegation is made because no such allegation is required to obtain mandamus relief as it would be in an election contest based on exploitation of the encryption keys. The Secretary must defend the case that was filed, not one he wishes had been filed.

Second, the cybersecurity threat to election systems is not a purely hypothetical concern, and it is flip and irresponsible for the Secretary to suggest that it is. The "Mueller Report's findings leave no doubt that Russia and other adversaries will strike

again." *Curling v. Raffensperger*, 702 F.Supp.3d 1303, 1360 (N.D. Ga. Nov. 10, 2023) (alterations and internal quotation omitted) As the Applicant's expert Ben Cotton described the encryption keys vulnerability in his declaration, "Simply put, this is like a bank having the most secure vault in the world, touting how secure it is to the public and then taping the combination in large font type on the wall next to the vault door." Application, Exh. 4, Cotton Affidavit, ¶ 19. The bank manager who did such a thing would be in gross dereliction of his duties even if no money were stolen. Complying with security procedures is a fundamental duty of those responsible for the operation of both banks and elections. Compliance with security requirements is not hypothetical. It is urgent, necessary and required.

The gravity of the cyber risk toe election systems prompted the Department of Homeland Security (DHS) Secretary Jeh Johnson to designate U.S. election systems as part of the nation's "critical infrastructure" in January, 2017. Critical infrastructure is a DHS designation for "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The designation was made in response to apparently foreign cyber-attacks on election systems. *See The Designation of Election Systems as Critical Infrastructure*, January 18, 2019, THE CONGRESSIONAL RESEARCH

SERVICE, available at https://crsreports.congress.gov/product/pdf/IF/IF10677/6 (last visited Sep. 27, 2024).

The outcome of U.S. presidential elections is of vital interest to sophisticated adversary nation states like China, Russia and Iran. We have already seen evidence of foreign cyber-attacks on U.S. election systems. *See, e.g.* CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY [CISA]Alert (AA20-304A), *Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data*, November 3, 2020, available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-304a (last visited Sep. 27, 2024). The sophistication and success of Chinese and Russian hacking of intensely guarded U.S. government computer systems is astounding. *See OPM Hack Far Deeper Than Publicly Acknowledged, Went Undetected For More Than A Year, Sources Say*, ABC NEWS, June 11, 2015, available at https://abcnews.go.com/politics/opm-hack-deeper-publicly-acknowledged-undetected-year-sources/story?id=31689059 (last visited Sep. 27, 2024) and *SolarWinds: Why the Sunburst hack is so serious*, December 15, 2020, BBC, available at https://www.bbc.com/news/technology-55321643 (last visited Sep. 27, 2024). These U.S. government networks are far more secure than Georgia's election systems – after all, they do not leave their encryption keys laying around in plain text – and they were deeply penetrated for extended periods without detection.

If compliance with security protocols were merely hypothetical, election systems would not have been designated as critical infrastructure, EAC certification of

compliance with the VVSG security requirements would not be required, ongoing compliance would not be required, and the contract between the State and Dominion would not require that the systems be secure and meet the applicable standards. The suggestion that the plaintext storage of the encryption keys is a minor and purely hypothetical problem cannot be taken seriously.

IV. MANDAMUS RELIEF IS AVAILABLE FOR A GROSS ABUSE OF DISCRETION.

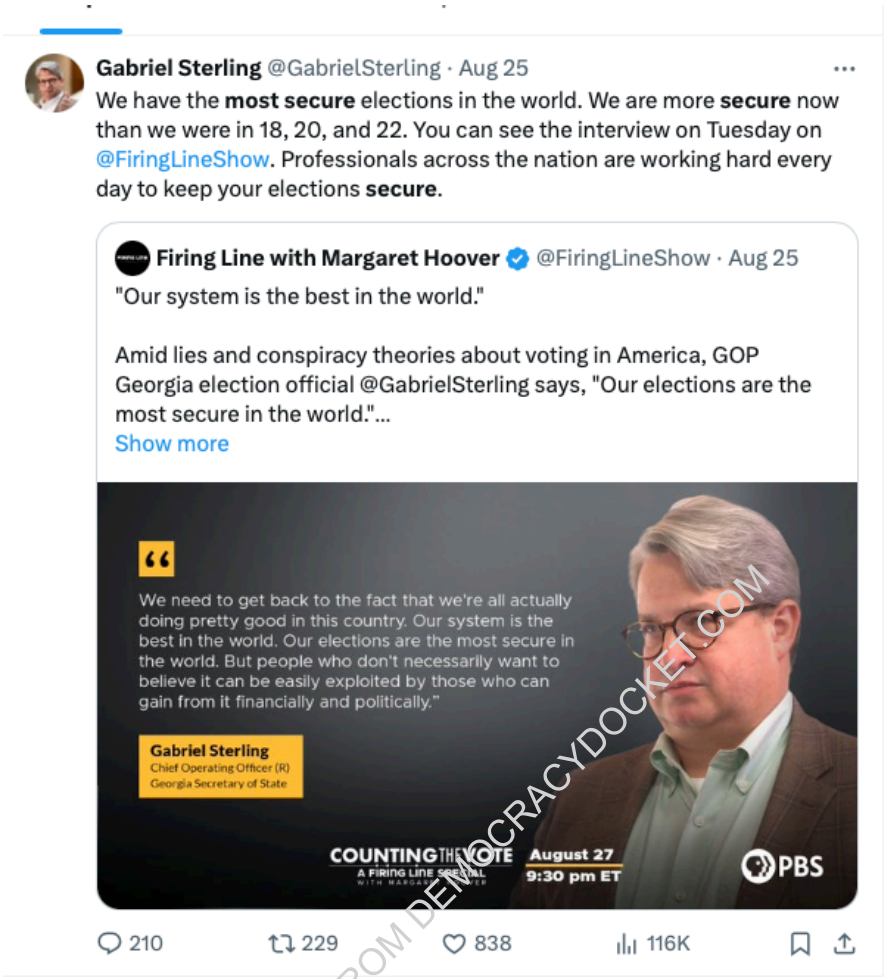
As noted above, Georgia law is crystal clear that mandamus is available to require the performance of discretionary duties where there has been a gross abuse of discretion: "Mandamus shall not lie as ... to a public officer who has an absolute discretion to act or not to act unless there is a ***gross abuse of such discretion***. However, mandamus ***shall not be confined to the enforcement of mere ministerial duties***." O.C.G.A. § 9-6-21(a) (emphasis added).

Here, the Secretary has grossly abused his discretion by forcing the use of systems that flagrantly fail to meet the applicable legal requirements for storage of the encryption keys as alleged in the Application and will be proven at the hearing.

The Secretary has known of this failure since no later than July 2021 when the Halderman Report, dated July 1, 2021, was delivered in *Curling v. Raffensperger*, U.S.D.C. N.D. Ga., Case No. 1:17-CV-2989-AT. Sections 6.1 and 9.1 of that report plainly describe that the encryption keys are stored in plain text in the election database and can be retrieved with a SQL query, an example of which was included in the report. *See*

Application for Mandamus Relief, ¶s 24-25. The report describes what is possible with access to the encryption keys: "As a result, anyone with access to the encryption key and IV discussed above can decrypt the ICX.dat file, modify it, and re-encrypt it using a command similar to the one shown above. My testing shows that the ICX will accept the modified file as if it were genuine." Halderman Report, p. 49. Halderman characterized the vulnerability as "an extremely dangerous approach to cryptographic design." *Id*. Despite receiving this report more than three years ago, the Secretary has done nothing.

In addition, the Secretary's General Counsel was also directly informed of the problem with the encryption keys and the additional element of noncompliance with the certification requirements in March of this year. *See* Exh. 5 to Application. Despite being on notice of the encryption key vulnerability since July 2021, and again having the noncompliance with certification requirements brought directly to the attention of the Secretary's General Counsel this past March, the Secretary has taken no remedial action whatsoever. Instead, knowing of this egregious cybersecurity weakness and of the noncompliance with certification requirements, the Secretary's press spokesman, Gabriel Sterling just last month was making public relations statements such as the following:



See https://x.com/GabrielSterling/status/1827856510967332942 (last visited Sept. 27, 2024). The statement by Mr. Sterling that Georgia has "the most secure elections in the world" must be viewed as uninformed and incorrect at best.

V. IF THE REQUESTED RELIEF IS NOT POSSIBLE FOR THE 2024 ELECTION, THE COURT SHOULD ORDER INTERIM MITIGATING RELIEF.

The Application requests certain interim and mitigating relief in paragraph 36 and 37. While no such argument is made in the MTD nor any such defense raised in the Answer, the Secretary may contend at the hearing that it is not practically feasible to implement secure storage of the encryption keys as required by FIPS 140-2, the VVSG,

EAC certification and O.C.G.A. § 21-2-300 in time for the November 2024 election. Such a defense would be based on O.C.G.A. § 9-6-26, which provides "Mandamus will not be granted when it is manifest that the writ would, for any cause, be nugatory or fruitless, nor will it be granted on a mere suspicion or fear, before a refusal to act or the doing of a wrongful act." If the Secretary proves that it is impossible to fix the encryption keys storage problem before the November 2024, then the DeKalb GOP is entitled to interim and mitigating relief as prayed for in the Application in paragraphs 36 in the form of prompt availability of the system logs, the Cast Vote Record and the ballot images, and in paragraph 37 in the form of compliance with Georgia State Election Board Rule 183-1-12-.12 *Tabulating Results*. "[M]andamus shall not be confined to the enforcement of mere ministerial duties." O.C.G.A. § 9-6-21(a). The interim and mitigating relief prayed for is entirely feasible as the records are already created and maintained by the election systems in the normal course of election administration and would pose no undue burden on election officials.

Furnishing these materials and complying with the Rule would ameliorate the risk arising from the Secretary's breach of his legal duty with respect to secure storage of the encryption keys in two ways. First, the requested materials will enable detection of certain categories of significant irregularities on a timely basis. Second, the knowledge additional scrutiny of election integrity will be applied will serve not only to deter wrongdoing but also to improve public confidence in Georgia's elections. The

Secretary should have ordered at least these measures himself rather than simply doing nothing in the face of the encryption keys vulnerability.

VI. MANDAMUS RELIEF SHOULD BE GRANTED FOR FUTURE ELECTIONS.

Even if the Secretary cannot bring Georgia's election systems into compliance with FIPS 140-2, the VVSG, EAC certification and O.C.G.A. § 21-2-300 in time for the November 2024 election, he can certainly do so before the elections that follow in 2025, 2026 and 2028. Therefore, merely showing that he cannot cure his dereliction of his duty for the November 2024 election does not moot the claim for mandamus relief.

VII. THERE IS NO GROSS LACHES SUFFICIENT TO BAR MANDAMUS.

The Secretary contends that Applicant's claims are barred by laches. The argument is without merit because it misstates the law and the facts, such as they are in the procedural posture of a motion to dismiss.

1. THE MEANING OF "GROSS LACHES."

To begin, the legal standard is gross laches, not ordinary laches. Before *Marsh v. Clarke Cnty. Sch. Dist*., 292 Ga. 28 (2012), Georgia law had conflicting lines of authority, one holding that gross laches was a defense to mandamus, and another holding that laches in any form was categorically not defense to mandamus. *Id*. at 29-30. *Marsh* resolved the conflict in favor of the former position: "we conclude that the first line of cases, spawned by *Mayor & Alderman of Savannah v. Green,* [4 Ga. 26(3) (1848)] *supra*, sets forth the correct rule, i.e., that a mandamus action can be barred by gross laches." *Id*. at

30. The Secretary cites *Marsh* to argue that mandamus is barred by laches, MTD p. 20-21, but fails to accurately note that it must be "gross laches" to be a defense to mandamus.

The nature of "gross laches" sufficient to bar a claim for mandamus is far beyond the circumstances of this case. In *City of Savannah v. State ex rel. Green*, Justice Lumpkin, writing for the Court described gross laches as follows:

> One of the excuses assigned by the defendants below, for not performing the duty required by the Act was,—That the parties had slept on their right, if indeed they had any. It is certainly true, that the Court will not interfere by Mandamus, after considerable delay on the part of the party applying for it, ***and especially, if other interests have sprung up, which would be affected by the proceeding***. But the cases cited in support of this principle, show what is understood by the Courts as amounting to gross laches. In one, the applicant had slumbered from 1817 to 1829; and in the other from 1799 to 1813. *The King vs. The Stainforth and Headly Canal Company*, 1 M. & S. 32. *Rex vs. Commissioners of Cockermouth Inclosure* Act. 1 Barn. & Adolp. 378, 380. (Engl. Com. Law Rep. XX, 403.)

City of Savannah v. State ex rel. Green, 4 Ga. 26, 43 (1848) (emphasis added). Of course, no legitimate interests could have "sprung up" in reliance on the Secretary's breach of his duties under § 21-2-300(a). "To justify the court in refusing the writ of mandamus on the ground that the party applying has slept over his rights, the laches must be gross—the delay must be unreasonable." *Talmadge v. Cordell*, 167 Ga. 594, 146 S.E. 467, 471 (1928). In *S. Airways Co. v. Williams*, 213 Ga. 38, 38 (1957) the plaintiff sought a mandamus to require the Commissioner of Roads and Revenues to record a lease. Noting that "[t]here is a legal presumption, until the contrary appears, that a public

officer has regularly and properly performed his official duty," the Court rejected as "clearly" having "no merit" the defendant's contention that the plaintiff was chargeable with gross laches despite 16 years having passed from execution of the lease and the lawsuit where the plaintiff had no knowledge the lease had not been recorded.

2. THERE IS NO BASIS FOR A FINDING OF GROSS LACHES.

Having misstated the legal standard, the Secretary next argues that the Applicant's claim is barred by laches. The Secretary is in essence arguing that if he violates the law for a long enough time, his duty to comply can no longer be enforced. Apart from the illogic, this argument the Secretary mischaracterizes the facts.

As alleged in the Application, the Secretary was given the Halderman Report in July of 2021. Application, ¶ 24(c). The report was so sensitive it was immediately placed under seal and was not made available to the public until 2023.[1] *Id*. Instead, it was sent to CISA for their review and analysis. *Id*. When the report was finally unsealed after more than a year, it documented the encryption keys vulnerability but said nothing about certification requirements. Application, ¶ 24(c) and ¶ 26. Later, when CISA issued a bulletin recommending various security upgrades and remedial measures, it said nothing whatsoever about encryption keys, much less about certification standards for

[1] Jane C. Timm and Kevin Collier, *Expert report fuels election doubts as Georgia waits to update voting software*, NBC News, July 16, 2023, available at https://www.nbcnews.com/politics/2024-election/expert-report-fuels-election-doubts-georgia-waits-update-voting-softwa-rcna89566 (last visited Sep. 27, 2024).

the management and storage of encryption keys. *Id*. at ¶ 25, 27. Dominion later issued a software update but that too failed to address the encryption key vulnerability. *Id*. And, of course, the Secretary has done nothing to address either the encryption key vulnerability itself, or the Georgia election systems' noncompliance with certification requirements. Since these expert entities failed to address the encryption keys vulnerability and its implications for compliance with EAC certification requirements, there is no basis for charging the DeKalb GOP with gross laches for not noticing them either.

These warnings were not given to the DeKalb GOP, nor did it have any legal duty to monitor, heed, or correct them. Nor is there anything in the record to indicate that it was aware of them. These warnings were instead given to the Secretary who has the legal duty to monitor, heed, and correct them, but failed to do so. The DeKalb GOP was entitled to rely on the assumption that the Secretary would perform his legal duties. *S. Airways Co. v. Williams*, 213 Ga. at 38. The Secretary's laches argument would impose a greater duty of care on the DeKalb GOP than the law imposes on him, despite all of these prior notices being given directly to him. This is inverted and should be rejected.

The Secretary also contends that his breach of duty to field a system compliant with certification requirements was known to the Applicant for years. But there is nothing in the Application that shows this. Curiously, in making this argument the

Secretary never refers to the Halderman report, which he had for over a year before it was made public. His answer says only that the Halderman report speaks for itself, leaving unanswered whether he listened. Instead, the motion says that the Applicant has had the election databases for at least two years. There is nothing in the record evidence to support this contention that these records were in the possession of the DeKalb GOP during this period. While not on the face of the Application or the attachments, the evidence at trial will show that it was not the DeKalb GOP, but a different organization, VoterGA, that made open records act requests to all Georgia counties and received election databases from four of them and posted all the records received on a website. None of that proves that the DeKalb GOP was aware of the encryption keys issue nor of the failure of the Secretary to field a system that complies with the certification requirements.

3. THE SECRETARY'S ARGUMENTS ABOUT NON-PARTY LITIGATION IN OTHER JURISDICTIONS ARE FALSE AND IRRELEVANT.

The Secretary also contends that co-counsel for the Applicant Mr. Olsen knew about the encryption keys before, engaged in litigation over them, lost, and was sanctioned. The Secretary's contentions are false and irrelevant for at least six reasons.

First, assuming *arguendo* that a court in another jurisdiction had indeed ruled on the merits of the encryption issues raised in the Application, that would not control this Court's consideration of the issues as applied to DeKalb GOP: "In no event ... can issue preclusion be invoked against one who did not participate in the prior adjudication"

Baker v. General Motors Corp., 522 U.S. 222, 237-38 & n.11 (1998); *Pike Cty. v. Callaway-Ingram*, 292 Ga. 828, 832 (2013) (same). Any suggestion otherwise is frivolous.

Second, what Mr. Olsen knew and when he knew it is irrelevant to DeKalb GOP's knowing anything. As indicated in the prior section, DeKalb GOP was not on notice of the encryption-key issue until deciding to bring this suit in August of 2024, which provides no basis for laches, much less gross laches.

Third, the Secretary's contention that other courts have rejected these issues is simply false. In the *Lake-Finchem* litigation in the Ninth Circuit, Mr. Olson has contested the security of the Dominion systems in other litigation, but there has never been any ruling on the encryption keys vulnerability. The "cases [cited by the Secretary] cannot be read as foreclosing an argument that they never dealt with." *Waters v. Churchill*, 511 U.S. 661, 678 (1994) (plurality). To the contrary, those other decisions did not consider, much less decide these issues:

> Questions which merely lurk in the record, neither brought to the attention of the court nor ruled upon, are not to be considered as having been so decided as to constitute precedents.

Cooper Industries, Inc. v. Aviall Services, Inc., 543 U.S. 157, 170 (2004) (interior quotations omitted); *United States v. L. A. Tucker Truck Lines, Inc.*, 344 U.S. 33, 38 (1952) (where a point "was not there raised in briefs or argument nor discussed in the opinion of the Court," the prior "case is not a binding precedent on this point).

Fourth, even on failings of the Dominion machines other than the encryption keys, the final *Lake-Finchem* judgment dismissed the underlying litigation for lack of a sufficiently concrete and particularized injury (*i.e.*, standing) under Article III of the federal Constitution. *See Lake v. Hobbs*, 623 F. Supp. 3d 1015 (D. Ariz. 2022), *aff'd sub nom. Lake v. Fontes*, 83 F. 4th 1199, 1204 (9th Cir. 2023). A federal court's "threshold inquiry into standing in no way depends on the merits of the petitioner's contention that particular conduct is illegal." *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990) (internal quotation marks and alterations omitted); *Sierra v. City of Hallandale Beach*, 996 F.3d 1110, 1115 (11th Cir. 2021) ("a court cannot rule on the merits of a case after finding that the plaintiff lacks standing").

Fifth, although Mr. Olsen's team attempted in late March of this year to inject the encryption-key issue in connection with a petition for certiorari to the U.S. Supreme Court from the Ninth Circuit's affirming dismissal for lack of standing, that too is irrelevant to the merits here: "No proposition is more settled than that a denial of certiorari is not a statement on the merits." *United States v. Floyd*, 535 F.2d 1299, 1301 n.6 (D.C. Cir. 1976); *accord United States v. Carver*, 260 U.S. 482, 490 (1923) ("denial of a writ of certiorari imports no expression of opinion upon the merits of the case"); *Missouri v.*

Jenkins, 515 U.S. 70, 85 (1995) (*citing Carver*); *Brown v. Davenport*, 596 U.S. 118, 141-42 (2022) (denials of discretionary appellate review do not adjudicate the merits).[2]

Sixth, the Secretary's invocation of sanctions in *Lake v. Hobbs*, 643 F. Supp. 3d 989 (D. Ariz. 2022), is misleading in two additional respects beyond the fact that that case in district court did not involve encryption keys. First, the federal sanctions (also imposed on Professor Alan Dershowitz) are on appeal to the Ninth Circuit in *Lake v. Fontes*, Nos. 23-16022, 23-16023 (9th Cir.), so the Secretary should not have cited it as a final decision without noting the pending appeal. Second, in related proceedings before the Arizona Bar, Mr. Olsen and his co-counsel were charged with violating Rules 1.1 (competence), 1.3 (diligence), 3.1 (meritorious claims and contentions), 8.4(c) (conduct involving dishonesty, fraud, deceit, or misrepresentation), and 8.4(d) (conduct prejudicial to the administration of justice). These claims were dismissed after a three-day trial on the merits. *See In re Olsen*, No. PDJ 2024-9003 (Arizona Bar Aug 26, 2024); Stacey Barchenger, *Lake, Finchem attorneys cleared of ethics violations Had challenged use of voting machines in 2022*, THE ARIZONA REPUBLIC, at 1 (Aug 28, 2024) available at https://www.pressreader.com/usa/the-arizona-republic/20240828/281530821367916 (last

[2] After the Supreme Court denied review, Mr. Olsen sought to raise the encryption-key via a motion to recall the Ninth Circuit's mandate in the *Lake-Finchem* litigation, which the panel denied in a two-line order and likewise does not constitute any sort of adjudication of the merits.

visited Sep. 27, 2024). The Secretary is triply disingenuous in raising this irrelevant issue.

In summary, notice to Mr. Olsen of the certification aspect of the encryption keys vulnerability only dates back only to March of this year, is not attributable to the Applicant, and no court has decided any of these issues on the merits. By citing irrelevant decisions to mischaracterize the serious issues here as "false" a mere "narrative," and "the same discredited conspiracy theories," Mot. 1-2, 4, the Secretary opens the question of whether he honestly understands the issues here: "You keep using that word. I do not think it means what you think it means." THE PRINCESS BRIDE (1987) (available at http://www.imdb.com/title/tt0093779/quotes (last visited Sept. 27, 2024).

CONCLUSION

The Secretary's motion to dismiss is without merit. The argument that he has no ongoing duty to ensure that the system he requires be used in Georgia's election meets the cybersecurity certification requirements makes certification an empty and pointless gesture. The legislature required the Secretary to certify that the systems are "safe and practical for ***use***" in elections, not merely safe in a testing laboratory. To evade this duty, the Secretary builds and knocks down straw man arguments the Applicant does not make. We do not ask for the Secretary to second guess the EAC. We ask that he be ordered to perform his state law statutory duty to field a system that actually complies with the certification requirements in ongoing operations.

The Secretary also serially mischaracterizes the law. He argues the Court has no authority to remedy improper performance, contrary to the plain language of O.C.G.A. § 9-6-21 which authorize the Court to remedy "improper performance" and order the "due performance" to prevent a "defect of legal justice." He makes an absurd argument that an election contest is an adequate remedy at law when the DeKalb GOP cannot even legally file an election contest. He finally argues laches when his own hands are filthy and when the law requires gross laches to bar the claim. Lastly, he disingenuously smears opposing counsel with false and irrelevant citations to other litigation. There is no indication whatsoever of ordinary laches, much less gross laches.

The Secretary's motion to dismiss should be denied.

Respectfully submitted, September 28, 2024.

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

OLSEN LAW, P.C.

Kurt B. Olsen*
1250 Connecticut Ave., NW, Ste. 700

Washington DC 20036
(202) 408-7025
ko@olsenlawpc.com

** Pro Hac Vice Application pending*

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document on counsel of record by filing the same in the Court's electronic filing system which will cause electronic service to be made upon all such counsel of record.

September 28, 2024.

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