AMENDED EMERGENCY ADMINISTRATIVE PETITION TO VACATE CERTIFICATION OF DOMINION VOTING SYSTEMS DEMOCRACY SUITE 5.5-A AND FOR INTERIM RELIEF

The DeKalb County Republican Party, Inc. ("DeKalb GOP"), Voters Organized for Trusted Election Results in Georgia, ("VoterGA"), VoterGA's co-founder, Garland Favorito, Rick Armstrong, Earl T. Martin M.D., and David Oles (collectively, the "Georgia Petitioners") petition the Commissioners and Executive Director of the U.S. Election Assistance Commission ("EAC") to revisit EAC's certification of Dominion Voting System ("DVS") Democracy Suite 5.5-A based on new information that DVS Democracy Suite 5.5-A fails to meet EAC's certification standards. DeKalb GOP's technical experts testified that DVS Democracy Suite 5.5-A not only includes a hard-coded administrative password but also stores encryption keys in plain text. The experts—Clay Parikh and Benjamin Cotton—are highly experienced cybersecurity professionals, *see* Parikh Decl. at 1-2 (¶¶ 3-7) (Aug. 15, 2024) (Ex. A); Cotton Decl. at 1-2 (¶¶ 4-13) (Aug. 18, 2024) (Ex. B). Their testimony calls into question whether EAC ever should have certified DVS Democracy Suite 5.5-A as complying with EAC's certification requirements. Indeed, Mr. Parikh's experience includes certifying election systems under EAC's Voluntary Voting System Guidelines ("VVSG") working for an EAC-accredited voting system testing laboratory. Parikh Decl. at 2 (¶ 5). DeKalb GOP's experts testified that the foregoing two defects in DVS Democracy Suite 5.5-A violate EAC's certification standards in ways that allows anyone with access to the voting system complete and virtually undetectable control over election results, thereby making election results both vulnerable and untrustworthy. Parikh Decl. at 7 (¶ 25); Cotton Decl. at 6 (¶ 25). While it may be too late for EAC to act in advance of the 2025 election cycle, the urgency of these defects require EAC's attention and resolution before the 2026 election cycle.

As explained below, DeKalb GOP expeditiously sought to protect the right of its members and itself to fair elections through the Georgia court system against Georgia's Secretary of State. Unfortunately, due to a June 2025 "course correction" by the Georgia Supreme Court on the doctrine of "standing" to sue, the Georgia Court of Appeals dismissed DeKalb GOP's challenge based on a recent Georgia Supreme Court decision that changed the rules for establishing standing while DeKalb GOP's challenge was on appeal. To protect the safety of Georgia elections for the 2026 election cycle, the Georgia Petitioners therefore respectfully petition the EAC—both the full Commission and the Executive Director—to revisit EAC's certification of DVS Democracy Suite 5.5-A. VoterGA and more than forty county, district, and state political-party organizations joined *amicus curiae* briefs in support of DeKalb GOP's state-court effort. Like VoterGA, many of those political-party organizations may join the Georgia Petitioners before the EAC. By supplemental letter to EAC's General Counsel, we will update EAC when new individuals or entities join this administrative petition. In addition, the Georgia Petitioners expect that voters and entities from other states affected by other DVS Democracy Suite versions may file "me-too" petitions with EAC to address similar or identical election-integrity issues that affect them.

LEGAL BACKGROUND

Under the Administrative Procedure Act, 5 U.S.C. §§ 551-706 ("APA"), federal agencies review applications through informal adjudications under 5 U.S.C. §555. *See Pension Benefit Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 655-56 (1990) ("minimal requirements for [informal adjudication] are set forth in §555"). In addition to the initial processing of an application, that section requires agencies to provide the opportunity to revisit past determinations. 5 U.S.C. 555(b); *cf.* 5 U.S.C. 553(e) (similar for revisiting rules). In pertinent part, 5 U.S.C. 555(b) allows the affected public to present requests to federal agencies and requires the agency to respond:

> So far as the orderly conduct of public business permits, an interested person may appear before an agency or its responsible employees for the presentation, adjustment, or determination of an issue, request, or controversy in a proceeding, whether interlocutory, summary, or otherwise, or in connection with an agency function. With due regard for the convenience and necessity of the parties or their representatives and within a reasonable time, each agency shall proceed to conclude a matter presented to it.

5 U.S.C. § 555(b). Agencies must provide prompt notice of a denial and, unless self-explanatory, "the notice shall be accompanied by a brief statement of the grounds for denial." *Id.* § 555(e). An initial denial must include a "brief statement of the grounds for denial" if the "denial is [not] self-explanatory." 5 U.S.C. §555(e); *Roelofs v. Sec'y of Air Force*, 628 F.2d 594, 600 (D.C. Cir. 1980) ("legislative history of § 555(e) supports its applicability, and thus with the requirement of a statement of the basis for denying a request, even where there is no formal proceeding or hearing"). When an administrative petition presents new information or changed circumstances, an agency's decision not to reopen the matter is judicially reviewable. *ICC v. Bhd. of Locomotive Eng'rs*, 482 U.S. 270, 284-85 (1987) ("*BLE*").

When an agency takes otherwise-final action through a subordinate officer, appeal to the agency head is not required for judicial review. 5 U.S.C. § 704. But the APA allows such intra-agency appeals unless the implementing statute expressly prohibits them: "higher-level agency reconsideration by the agency head is the standard way to maintain political accountability and effective oversight for adjudication that takes place outside the confines of § 557(b)." *United States v. Arthrex, Inc.*, 594 U.S. 1, 20 (2021) (cleaned up).

In addition to seeking judicial review of final agency action, 5 U.S.C. § 706, the APA also contemplates interim relief, both from the agency itself and from a reviewing court:

> When an agency finds that justice so requires, it may postpone the effective date of action taken by it, pending judicial review. On such conditions as may be required and to the extent necessary to prevent irreparable injury, the reviewing court, including the court to which a case may be taken on appeal from or on application for certiorari or other writ to a reviewing court, may issue all necessary and appropriate process to postpone the effective date of an agency action or to preserve status or rights pending conclusion of the review proceedings.

5 U.S.C. § 705.

PROCEDURAL AND FACTUAL BACKGROUND

The pertinent background at EAC and in Georgia is as follows:

1. At all relevant times, Georgia law required Georgia's Secretary of State to obtain and provide to Georgia's counties an EAC-certified election system. O.C.G.A. § 21-2-300(a)(3); *cf.* O.C.G.A. § 21-2-50(b) (Secretary of State is Georgia's Chief Elections Official).

2. On January 30, 2019, EAC's then-Executive Director, Brian Newby, issued a Certificate of Conformance for DVS Democracy Suite 5.5-A.

3. Georgia certified the DVS Democracy Suite 5.5-A in August 2019 and has used DVS Democracy Suite 5.5-A in all state elections since then. Unless changed at the state level, Georgia will use DVS Democracy Suite 5.5-A in all future elections.

4. In August of 2024, DeKalb GOP was advised that, at all times relevant to this petition, DVS Democracy Suite 5.5-A not only included a hard-coded administrative password but also stored encryption keys in plain text.

5. On August 30, 2024, DeKalb GOP petitioned the Superior Court of Fulton County for a writ of mandamus to Georgia's Secretary of State to challenge Georgia's use of Democracy Suite 5.5-A in Georgia elections on the basis that Democracy Suite 5.5-A did not meet EAC certification requirements in use.

6. Georgia's Secretary of State defended the challenge on the merits by arguing that he complied with Georgia law because O.C.G.A. § 21-2-300(a) required only that the election system be an EAC-certified system, without regard to whether the election system met EAC's requirements when used in elections.

7. When DeKalb GOP petitioned for a writ of mandamus, Georgia precedent gave membership organizations like DeKalb GOP associational standing to sue on behalf of members, who are Georgia voters. Georgia law also recognized organizational standing.

8. In a decision dated October 4, 2024, the Fulton County Superior Court issued a merits decision agreeing with the Secretary of State's argument that O.C.G.A. § 21-2-300(a) imposed only a one-time requirement that Georgia's election systems be certified by the EAC, regardless of whether the election systems met EAC requirements when used in actual elections. *DeKalb Cty. Republican Party v. Raffensperger*, No. 24cv011028 (Fulton Cty. Super. Ct. Oct. 4, 2024).

9. DeKalb GOP appealed the denial of mandamus, and the parties' briefing in Georgia's Court of Appeals was completed with the filing of DeKalb GOP's reply brief on March 10, 2025.

10. On June 10, 2025, while DeKalb GOP was appealing the Superior Court's counterintuitive decision, Georgia's Supreme Court abolished associational standing in what the court described as a "course correction[]." *Republican Nat'l Comm. v. Eternal Vigilance Action, Inc.*, 321 Ga. 771, 776 (2025).

11. Without seeking additional briefing on the issue of organizational standing—which remains part of Georgia' standing doctrine, *id.* at 780 n.6—Georgia's Court of Appeals dismissed DeKalb GOP's appeal on the alternate ground that DeKalb GOP lacked organizational standing to

sue. *DeKalb Cty. Republican Party v. Raffensperger*, 2025 Ga. App. LEXIS 400, at *7 (Ct. App. Sep. 19, 2025) (No. A25A0831).

12. Although DeKalb GOP believes it has or could establish institutional standing based on its own interests in fair elections—notwithstanding that *Eternal Vigilance* now precludes relying on members' interests—that path would likely be fruitless because appeal of the Court of Appeals' dismissal to Georgia's Supreme Court would address the standing issue, not the merits. Relief on the merits would have to await a remand from the Georgia Supreme Court back to the Court of Appeals to address the merits. In short, the Georgia court system appears unable to provide DeKalb GOP—and its members—any relief in advance of the 2026 election cycle.

13. Rather than pursue that appellate option, DeKalb GOP and the other Georgia Petitioners now challenge the EAC decision to certify DVS Democracy Suite 5.5-A in the first place.

14. In 2005, EAC adopted its VVSG in a two-volume set. EAC, *Voluntary Voting System Guidelines*, vol. I-II (2005).

15. On February 10, 2021, the EAC's Commissioners unanimously adopted the newest VVSG standard, version 2.0. EAC, U.S. Election Assistance Commission Adopts New Voluntary Voting System Guidelines 2.0 (Feb. 10, 2021) (https://www.eac.gov/news/2021/02/10/us-election-assistance-commission-adopts-new-voluntary-voting-system-guidelines-20 (last visited Oct. 30, 2025).

16. On June 16, 2023, EAC issued guidance on the transition to VVSG version 2.0. *See* EAC, *Voting System Testing and Certification: VVSG Lifecycle Policy* (June 16, 2023) (https://www.eac.gov/sites/default/files/TestingCertification/VVSG_Lifecycle_Policy_9_22.pdf (last visited Oct. 30, 2025).

17. On July 17, 2025, on a page entitled "Voluntary Voting System Guidelines (VVSG) Migration," EAC summarized its migration plans for phasing our VVSG version 1.0 and 1.1 and requiring compliance with VVSG version 2.0:

> **VVSG 1.0 and 1.1 Certified Voting Systems Will Continue to be Certified and Secure**
>
> All EAC-certified voting systems, no matter if they are certified to VVSG 1.0 or 1.1, are secure. Election officials may still use or procure systems that have been certified to VVSG 1.0 and 1.1 unless otherwise dictated by individual state statute.
>
> The EAC ceased accepting applications for voting systems to be tested against VVSG 1.0 and 1.1 on November 15, 2023. , VVSG 1.0 and 1.1 are now no longer be used by the EAC to certify voting systems, and all applications for voting systems to be newly certified by the EAC must be for VVSG 2.0. Limited maintenance modifications to existing EAC-certified (version 1.0 and 1.1) systems may be continued to be tested and certified.

> **Migration of Voting Systems Certified to VVSG 1.0 and 1.1.**
>
> Voting systems are not decertified by the EAC as the result of VVSG migration. Election officials may continue to use or procure voting systems that have been certified to VVSG 1.0 and 1.1 in accordance with state or local law.
>
> **Path to VVSG 2.0 Certification for New Voting Systems**
>
> Adopting the VVSG 2.0 is an important step to enhance U.S. election security, which is a national security imperative. With the accreditation of both Voting System Test Labs (VSTL) in November and December 2022, the EAC is now accepting voting systems for testing towards VVSG 2.0.
>
> Currently, there is one voting systems certified to VVSG 2.0. It will take time for new systems to be developed, certified, and fielded for use in elections, particularly in an environment of constrained funding for state and local election offices. As of January 2024, three systems have been submitted to the EAC and are currently being tested to VVSG 2.0.

https://www.eac.gov/election-officials/voluntary-voting-system-guidelines-vvsg-migration (last visited Oct. 30, 2025) (emphasis in original).

18. Under the circumstances, EAC should determine DVS Democracy Suite 5.5-A's entitlement to certification under version 1 of the VVSG and—to the extent that DVS Democracy Suite 5.5-A fails that test—EAC presumably should determine DVS Democracy Suite 5.5-A's entitlement to recertification under version 2 of the VVSG.

19. On its "Certified Voting Systems" page, EAC describes the VVSG's central role in the certification process as follows:

> 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.

https://www.eac.gov/voting-equipment/certified-voting-systems (last visited Oct. 30, 2025); *accord Voluntary Voting System Guidelines*, vol. I, at x (2005) ("The VVSG specifies the functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the national certification of voting systems.") (emphasis omitted).

20. VVSG 1.0 requires manufacturers to provide purchasing jurisdictions with voting systems capable of adhering to and enforcing operational procedures such as "effective password management." *Voluntary Voting System Guidelines*, vol. I, at 114 (§ 7.1.1) (2005). It also identifies passwords as "information that needs to be protected" during transmissions, *id,* at 132 (§ 7.7.3), and recommends a Federal Information Processing Standards Publication—*Password Usage*

(FIPS 112)—as an additional reference that is "useful in understanding and complying with the [VVSG]." *Id.* at B-7 (Appendix B.4).

21. Sections 3.3 through 3.7 of Federal Information Processing Standards ("FIPS") for password usage include requirements for password strength, lifetime, origination, ownership, distribution, and storage. *See* National Institute of Standards and Technology, *Password Usage*, at 11-12 (FIPS PUB 112 May 30, 1985).

22. VVSG 1.0 also specifically includes requirements for data encryption, which include the adoption of FIPS standards as mandatory practices for protection of cryptographic keys. Specifically, the VVSG requires "cryptographic keys … use a FIPS 140-2 level 1 or higher validated cryptographic module." *Voluntary Voting System Guidelines*, vol. I, at 122 (§ 7.4.5.1(a)(i)) (2005) (Hashes and Digital Signatures); *see also id.* at 125 (§ 7.5.1(b)(i)) (Maintaining Data Integrity); *id.* at 132 (§ 7.7.3(a)(ii)) (Protecting Transmitted Data); *id.* at 138 (§ 7.9.3) (Electronic and Paper Record Structure subsection a).

23. Section 4.7 of FIPS 140-2 "Cryptographic Key Management" states the "security requirements for cryptographic key management encompass the entire lifecycle of cryptographic keys[.]" National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, at 30 (FIPS PUB 140-2 May 25, 2001). The section also states that "Secret keys, private keys, and CSPs shall be protected within the cryptographic module from unauthorized disclosure, modification, and substitution." *Id.* Section 4.7.5 "Key Storage" states "Plaintext secret and private keys shall not be accessible from outside the cryptographic module to unauthorized operators." *Id.* at 33. Additionally, the National Institute of Standards and Technology NIST SP 800-5716 section 4.7 "Key Information Storage" states that "[t]he integrity of all key information **shall** be protected; the confidentiality of secret and private keys and secret metadata **shall** be protected. When stored outside a cryptographic module[.]" National Institute of Standards and Technology, *Recommendation for Key Management: Part 2–Best Practices for Key Management Organizations*, at 43 (NIST Special Publication 800-57 Part 2 Revision 1, May 2019) (emphasis in original).

24. On December 12, 2018, SLI Compliance submitted Release 1.2 of the test plan for DVS Democracy Suite 5.5-A to EAC for review.

25. On information and belief, Release 1.2 of the test plan for DVS Democracy Suite 5.5-A neither indicated nor tested for DVS Democracy Suite 5.5-A's including a hard-coded administrative password or DVS Democracy Suite 5.5-A's storing encryption keys in plain text.

26. By letter dated December 12, 2018, in his capacity as EAC's Director for Testing and Certification, Brian J. Hancock approved Release 1.2 of the test plan for DVS Democracy Suite 5.5-A. In that letter, Mr. Hancock indicated that EAC's approval was "based on information submitted" and that EAC did "not know[] if relevant information was omitted that would affect the testing campaign."

27. The facts that DVS Democracy Suite 5.5-A included a hard-coded administrative password and that DVS Democracy Suite 5.5-A stored encryption keys in plain text would have been material to EAC's review of Release 1.2 of the test plan for DVS Democracy Suite 5.5-A and

to EAC's decision to certify DVS Democracy Suite 5.5-A. Specifically, EAC would neither have approved the test plan nor have certified the election system if EAC had known of those security flaws.

28. Mr. Hancock's letter dated December 12, 2018, also indicated that the "test plan is a living document and is expected to change and be updated during various phases of the testing life cycle" and that "EAC reserves the right to request further updates to the test plan and possibly additional testing" if the "final 'as run' test plan does not reflect all the testing required."

29. On January 30, 2019 (*i.e.*, the same day EAC issued a Certificate of Conformance for DVS Democracy Suite 5.5-A), then-Executive Director Newby's letter conveying the certification indicated that "the manufacturer accepts the certification and all conditions placed on the certification."

30. EAC's Certificate of Conformance for DVS Democracy Suite 5.5-A included a Scope of Certification. That Scope of Certification included a section captioned "Functionality," which indicates "YES" for the line item "FIPS 140-2 validated cryptographic module."

31. Among the conditions placed on submissions to federal agencies is the duty not to submit false or misleading information, 18 U.S.C. §§ 1001(a), 1519, which includes a duty to correct material information previously submitted that one later learns to have been false.

32. VVSG 1.0 requires ongoing compliance with certification standards. *See Voluntary Voting System Guidelines*, vol. I, at 147 (§ 8.1) (2005) (discussing the conforming the system to meet VVSG and state and local requirements throughout the life of the system); *cf. id.* at 155 (§ 9.5) (discussing establishment of procedures to resolve identified defects).

33. After analyzing an authenticated copy of an EAC-certified Election Management Server ("EMS") for a Georgia county and similar servers in other states, DeKalb GOP's experts testified that—in all systems and states analyzed—DVS Democracy Suite 5.5-A not only includes an unchanged, hard-coded administrative password but also stores encryption keys in easily retrievable plain text. *See* Parikh Decl. at 3-7 (¶¶ 13-24); Cotton Decl. at 3-4 (¶¶ 17-20); Tr. 91:20-92:9, 92:14-93:7, 93:21-94:9, 109:24-112:10, 124:16-125:6, 127:1-128:2, 133:3-134:14, 138:14-139:15, 192:17-193:3, 205:9-13, 248:13-249:4, 250:18-251:1 (Sept. 30, 2024), *DeKalb Cty. Republican Party v. Raffensperger*, No. 24cv011028 (Fulton Cty. Super. Ct.) (Ex. C).

34. A declaration from a computer expert unaffiliated with DeKalb GOP also identified the encryption key vulnerability of DVS Democracy Suite 5.5-A. *See* Prof. J. Alex Halderman, Ph.D., *Security Analysis of Georgia's ImageCast X Ballot Marking Devices*, at 48-49 (July 1, 2021) (unsealed in redacted form June 14, 2023), *Curling v. Raffensperger*, No. 1:17-cv-02989-AT (N.D. Ga.) (Ex. D); *see also* Tr. 52:23-53:1 (discussing Halderman report).

35. Significantly, the use of hard-coded passwords was identified more than 10 years ago as an EAC testing deficiency of the DVS Democracy Suite 4.0 by Wylie Labs. *See* Wylie Test Report No. T57381-01 Appendix A.11 Deficiency Report, at 9 (undated) ("Hard coded Passwords

and hard coded Crypto Keys");[1] *see also* Tr. 124:17-125:6 (discussing deficiency identified in Wylie deficiency report).

36. Mr. Parikh testified that DVS Democracy Suite 5.5-A and other versions of the DVS Democracy Suite systems are remotely interconnectable and accessible worldwide because they use a common shared key value in X.509 Certificates. Tr. 116:5-117:10, 192:9-16, 255:25-257:19; *see also id.* at 256:11-13 ("that 509 value is the same in every single Dominion system that I've looked at regardless of version and regardless of jurisdiction").

37. DeKalb GOP's experts further established that the components within DVS Democracy Suite 5.5-A and other DVS versions are configured to be accessed remotely when installed. These include database remote configuration and installation of an uncertified data manipulation tool SQL Server Management Studio ("SSMS") Tr. 121:18-122:13, 198:18-199:9, 258:14-259:8.

38. Mr. Parikh further testified that he was aware of Dominion emails obtained through discovery in other cases in which he participated and that those emails establish that Dominion programmers accessed election servers in Georgia and another state during the 2020 election. Tr. 211:15-212:10, 258:23-259:4.

39. DeKalb GOP's experts classified DVS Democracy Suite 5.5-A's security as "egregious" and "inexcusable," Parikh Decl. at 4 (¶¶ 15), "horrendous," Tr. 251:1 (Cotton), and mind blowing, Tr. 111:9 (Parikh).

40. Mr. Cotton analogized DVS Democracy Suite 5.5-A's security defects as a bank's posting the combination to its safe on the wall next to the safe's door:

> 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.

Tr. 264:5-16. In short, DeKalb GOP's experts classified DVS Democracy Suite 5.5-A as remarkably insecure.

41. DeKalb GOP's experts testified that bad actors with access to the encryption keys could "do anything" with respect to the election, likely without detection:

[1] Appendix A.11 of Wylie Labs' Test Report No. T57381-01 is available on EAC's website at https://www.eac.gov/sites/default/files/voting_system/files/Dominion_Deficiency_Report.pdf (last visited Oct. 30, 2025).

> [T]hey can do anything. They can decrypt the configuration files which are -- for example, the tabulator components, and so I could make the tabulator -- they could easily manipulate that and make it do whatever.· They can decrypt the information coming back to the election management system -- the EMS.· They can manipulate the ballot images, they can manipulate the cast vote record, they can do any number of things.

Tr. 92:1-9; *see also* Tr. 127:22-128:2 (administrative password means "[one] could basically do anything [he or she] wanted to"); Tr. 134:18-137:24 (encryption keys allow bad actors to modify election results without detection); Tr. 156:17-25 ("If you do some of these vulnerabilities there will be no detection, especially in a system that does not upsize the logging information and constantly overrides the Windows logs."); Tr.160:3-4 ("I and Dr. Halderman have said there will be no evidence").

42. Mr. Parikh demonstrated these vulnerabilities in Fulton County Superior Court using an authenticated copy of a 2020 Georgia EMS, the same version that is still in use today in Georgia and that is currently expected to be used for the 2026 election cycle. He was able to move 1,000 or more Presidential race votes from one candidate to another during a 3-minute demonstration with only 6 lines of stored procedure code. Tr. 135:24-137:15.

43. In his analysis of the authenticated Georgia EMS, Mr. Cotton found that an uncertified compiler and SSMS data manipulation programs had been installed on the authenticated Georgia EMS. The compiler allows election program files to be added, changed, or replaced, in some instances without detection. Tr. 273:21-276:14.

44. Mr. Cotton further found over 3,000 Dominion program files had been modified without detection since the DVS Democracy Suite 5.5A system has been installed. Georgia election officials do not have the expertise to write the code for 3,000 program files, compile the code for those 3,000 program files, and integrate the code with the remaining programs in the Dominion software system. Tr. 279:25-282:25.

45. On September 13, 2024, in his capacity as the Chair of the Committee on House Administration, Rep. Bryan Steil wrote to EAC's Chair and Vice Chair to inquire about EAC's position on various issues related to DeKalb GOP's suit. That letter indicated that the "Committee thus seeks information on whether the allegations set out in the DeKalb County Republican Party's lawsuit are of valid concern" and asked a series of nine specific questions.

46. By letter dated September 23, 2024, EAC's Chair and Vice Chair responded to Chairman Steil that "EAC certification of a voting system does not expire, and a system can only lose its certification if the EAC formally decertifies it" and that "Dominion Democracy Suite 5.5-A voting system utilizes a Federal Information Processing Standards (FIPS) 140-2 cryptographic module for transmission of data between system components as required by the Voluntary Voting System Guidelines 1.0 (VVSG 1.0)," but also acknowledged that "[t]he integrity and security of encryption keys are essential in ensuring the protection of data transmitted between system components" and that while "EAC certifies voting systems as compliant with the VVSG," the "implementation is specifically left to the states."

47. Significantly, EAC's response to Rep. Steil did not address the issues raised in this petition—namely, whether DVS Democracy Suite 5.5-A included a hard-coded administrative password and whether DVS Democracy Suite 5.5-A stored encryption keys in plain text—because the nine questions in Rep. Steil's letter did not cover those issues. Unlike the issues to which EAC responded, the issues raised in this petition fall within EAC's certification process, not the states' implementation.

48. Under the circumstances, EAC appears not to have previously considered whether DVS Democracy Suite 5.5-A included a hard-coded administrative password and whether DVS Democracy Suite 5.5-A stored encryption keys in plain text. As such, this petition raises "new information" within the meaning of the *BLE* line of cases.

Further facts are set forth as their relevance arises in the body of this petition.

ARGUMENT

As explained below, the information supplied to DeKalb GOP by its experts indicates that DVS Democracy Suite 5.5-A never met EAC's VVSG security requirements and should not have been certified in its current form. Although the exchange of letters between Rep. Steil and EAC's Chair and Vice Chair identified some issues outside of EAC's control where state and local governments using DVS Democracy Suite 5.5-A could avoid *contributing* to election insecurity, the letters did not address the core issue of DVS Democracy Suite 5.5-A's using hard-coded administrative password and storing encryption keys in plain text. Those two issues fall within EAC's control and must be addressed.

EAC should determine whether DVS Democracy Suite 5.5-A met VVSG 1.0 when EAC certified DVS Democracy Suite 5.5-A.

As explained in Paragraphs 30 and **Error! Reference source not found.**-41, *supra*, there are two seemingly inconsistent facts. First, EAC's certification indicates that DVS Democracy Suite 5.5-A complied with FIPS 140-2 for encryption keys. *See* Paragraph 30, *supra*. Second, DeKalb GOP's experts indicate that DVS Democracy Suite 5.5-A not only includes a hard-coded administrative password but also stores encryption keys in plain text. *See* Paragraph **Error! Reference source not found.**-41, *supra*. Delivering a hard coded administrative password that remains unchanged and improperly unprotected during delivery and backup transmissions violates FIPS-112 and VVSG criteria for password protection, life, sourcing, distribution, and effective password management. *See* Paragraphs 20-21, *supra*. Storing encryption keys in an election database as easily accessible plain text clearly violates FIPS 140-2 and thus also violates the VVSG certification criteria. *See* Paragraphs 22-23, *supra*. EAC staff can and should expeditiously determine the facts that underlie this petition. It should be a straightforward task for EAC staff to determine two things:

- Whether DeKalb GOP's experts are correct that DVS Democracy Suite 5.5-A not only includes a hard-coded administrative password but also stores encryption keys in plain text.

- Whether evidence supports EAC's 2019 certification that DVS Democracy Suite 5.5-A complied with FIPS 140-2 for the encryption keys.

Once EAC has the answers to those two straightforward inquiries, EAC can proceed to respond to this administrative petition.

The Executive Director must reconsider DVS Democracy Suite 5.5-A's certification or—alternatively—consider whether to vacate it.

Now that the Georgia Petitioners have provided EAC with new information to suggest that EAC's Executive Director erred in certifying DVS Democracy Suite 5.5-A in 2019, EAC's current Executive Director has a clear APA duty to resolve expeditiously whether DeKalb GOP's new information changes the EAC's 2019 conclusion that DVS Democracy Suite 5.5-A complies with EAC's certification requirements. *See* 5 U.S.C. § 555(b). Whether or not EAC concurs with DeKalb GOP's new information, EAC's response to this petition should include an explanation of the basis for EAC's conclusion. *See* 5 U.S.C. § 555(e). Even if EAC declines to reopen its 2019 certification, EAC should explain its rationale to avoid unnecessary suspicion and to provide the opportunity to avoid otherwise-unnecessary litigation. *See BLE*, 482 U.S. at 284-85 (EAC's rejection of new information would be reviewable final action).

The EAC Commissioners must review DVS Democracy Suite 5.5-A's initial certification.

For the same reasons that EAC's Executive Director should revisit his predecessor's action in certifying DVS Democracy Suite 5.5-A, EAC's Commissioners should consider whether to reverse that certification as an appeal to the agency head: "higher-level agency reconsideration by the agency head is the standard way to maintain political accountability and effective oversight for adjudication that takes place outside the confines of § 557(b)." *Arthrex*, 594 U.S. at 20 (cleaned up). Neither the relevant statutes nor EAC's regulations purport to set a statute of limitations or other timeline on administrative appeals, and DeKalb GOP cannot be faulted under laches or a similar doctrine of prejudicial delay. DeKalb GOP acted quickly upon learning of the threat to Georgia's election integrity and acts quickly now upon the dismissal of its suit based on a judicial about-face on standing. Moreover, all the affected third parties—*e.g.*, Dominion Voting Systems, Georgia's Secretary of State—have known about these issues for as long or longer than DeKalb GOP. Laches requires clean hands, and none of the relevant third parties have clean hands here.

Although DeKalb GOP's administrative appeal to EAC's Commissioners relies on information that EAC's Executive Director did not consider in 2019, that is no obstacle to the Commissioners' including DeKalb GOP's new evidence in their review. The APA allows *de novo* judicial review for adjudications with deficient fact-finding. 5 U.S.C. § 706(2)(F); *Citizens to Preserve Overton Park, Inc. v. Volpe,* 401 U.S. 402, 415 (1971) ("*de novo* review is authorized when the action is adjudicatory in nature and the agency fact finding procedures are inadequate"); *Porter v. Califano*, 592 F.2d 770, 782-83 (5th Cir. 1979). Here, EAC made no effort whatsoever to seek public input, but the opportunity to comment is fundamental. *CNA Fin. Corp. v. Donovan*, 830 F.2d 1132, 1159-60 (D.C. Cir. 1987). It would be beyond strange if the Commissioners could not consider DeKalb GOP's new information, but a reviewing court were free to do so. Alternatively, if the Commissioners find DeKalb GOP's new evidence credible enough to warrant review by staff, the Commissioners could implement the interim relief explained below and direct the Executive Director expeditiously to review whether to reconsider or vacate DVS Democracy Suite 5.5-A's certification.

DVS Democracy Suite 5.5-A's severe security flaws require urgent action.

The urgency of this petition cannot be overstated. DeKalb GOP's experts demonstrated that DVS Democracy Suite 5.5-A is not only insecure *vis-à-vis* EAC's certification standards, *see* Paragraphs 20-23, **Error! Reference source not found.**-41, *supra*, but also can be and apparently has been impermissibly altered. *See* Paragraphs 42-44, *supra*. Consequently, DVS Democracy Suite 5.5-A is unfit for use in elections. Georgia's primary elections are scheduled for May 19, 2026. To give Georgia's Secretary of State and Georgia counties six months to develop alternate plans for the 2026 election, the Georgia Petitioners ask EAC to issue final action on this petition by November 20, 2025. If EAC cannot take final action in that timeframe, the Georgia Petitioners ask EAC to issue the interim relief that the APA contemplates: namely, to change the effective date of DVS Democracy Suite 5.5-A's certification sufficiently into the future to ensure that DVS Democracy Suite 5.5-A is not certified for—and therefore cannot be used in—the 2026 election cycle.

Before determining whether to vacate DVS Democracy Suite 5.5-A's certification, EAC should issue interim relief.

In the interest of justice, the APA allows an agency or a reviewing court to issue interim relief while a matter is pending before the agency or in court. 5 U.S.C. § 705. Here, the right to vote "is regarded as a fundamental political right, because preservative of all rights." *Yick Wo v. Hopkins*, 118 U.S. 356, 370 (1886), which should warrant issuance of interim relief if EAC's review concurs with DeKalb GOP's experts on the insecurity of DVS Democracy Suite 5.5-A. As with many things, interim relief presents an easy way and a hard way:

- It would be easy for EAC to determine that DVS Democracy Suite 5.5-A is insecure for use in elections and therefore to impose the interim relief that the APA itself suggests (*i.e.*, postponing the effective date of EAC's certification to after the 2026 elections). *See* 5 U.S.C. § 705. That would preclude use of DVS Democracy Suite 5.5-A in elections unless and until the manufacturer cured any deficiencies in its implementation of FIPS 140-2 for encryption keys and hard-coded passwords.

- As EAC's Chair and Vice Chair made clear in their response to Rep. Steil, it would be hard (and maybe impossible) for EAC to compel the use of curative interim measures (*e.g.*, the outputting and publication of system logs and election data during an election) to allow review to ensure that election data or parameters were impermissibly accessed or altered during the election. In addition to falling outside EAC's authority to impose, development of best-practice guidelines for that type of interim relief would involve more effort on the part of EAC and stakeholders to develop than simply postponing the effective date of the EAC certification of DVS Democracy Suite 5.5-A.

The Georgia Petitioners respectfully submit that the easy option is the appropriate choice because it puts the burden where it belongs (*i.e.*, on the manufacturer to cure the problem expeditiously), rather than putting the burden on EAC staff.

REQUESTED RELIEF

Under 5 U.S.C. §§ 553(e), 555(b), and 705, EAC—through either or both the Executive Director or the Commissioners—should revisit the certification of DVS Democracy Suite 5.5-A and—if that review determines that DVS Democracy Suite 5.5-A includes a hard-coded administrative password and stores encryption keys in plain text—issue the following corrective action:

- The Executive Director should reconsider the certification of DVS Democracy Suite 5.5-A and, on reconsidering that certification, vacate the certification of DVS Democracy Suite 5.5-A by November 20, 2025, based on the new evidence set forth herein. 5 U.S.C. § 553(b); *BLE*, 482 U.S. at 284-85.

- Wholly apart and independent from the Executive Director's reconsidering certification of DVS Democracy Suite 5.5-A, EAC's Commissioners should review the initial certification as an appeal of the Executive Director's 2019 decision, *Arthrex*, 594 U.S. at 20, and deny the certification *ab initio* by November 20, 2025.

- Alternatively, prior to November 20, 2025, pursuant to 5 U.S.C. § 705,EAC—through either or both its Executive Director and its Commissioners—should amend the effective date of DVS Democracy Suite 5.5-A's certification to January 15, 2027, to avoid any use of DVS Democracy Suite 5.5-A in the 2026 elections unless and until the EAC recertifies DVS Democracy Suite 5.5-A as affirmatively meeting EAC certification standards.

Although the relief requested does not require public input any more than the initial certification required public input, EAC should not delay promulgating interim relief for an extended public-comment period.

CONCLUSION

Acting through either or both its Executive Director or its Commissioners, EAC must revisit the certification of DVS Democracy Suite 5.5-A and adopt interim relief to protect against any risk of harm from the use of DVS Democracy Suite 5.5-A in U.S. elections.

Dated October 30, 2025

Respectfully submitted

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

Counsel for Petitioners

EXHIBIT A

Affidavit of Clay U. Parikh

EXHIBIT
3

Affidavit of Clay U. Parikh

1. I am over twenty-one (21) years of age, under no legal disability, and am otherwise competent to give this affidavit.

2. The matters sworn to herein are based on my personal knowledge.

3. I have a Master of Science in Cyber Security, Computer Science from the University of Alabama in Huntsville. I have a Bachelor of Science in Computer Science, Systems Major from the University of North Carolina at Wilmington. In February 2007 I obtained the Certified Information Systems Security Professional (CISSP) certification and continually maintained good standing, until I released it on 28 February 2024. I also held the following certifications: Certified Ethical Hacker (CEH) and Certified Hacking Forensic Investigator (CHFI).

4. Since December of 2003, I have continually worked in the areas of Information Assurance (IA), Information Security and Cyber Security. I have performed and led teams in Vulnerability Management, Security Test and Evaluation (ST&E) and system accreditation. I have supported both civil and Department of Defense agencies within the U.S. government as well as international customers, such as NATO. I have served as the Information Security Manager for enterprise operations at Marshall Space Flight Center, where I ensured all NASA programs and projects aboard the center met NASA enterprise security standards. I was also responsible in part for ensuring the Marshall Space Flight Center maintained its Authority to Operate (ATO) within the NASA agency. I have also served as the Deputy Cyber Manager for the Army Corps of Engineers where I led and managed several teams directly in: Vulnerability Management, Assessment and Authorization (A&A), Vulnerability Scanning, Host Based Security System (HBSS), Ports Protocols and Service Management, and an Information System Security Manager (ISSM) team for cloud projects. I also have performed numerous internal digital forensic audits. During this time span, I also worked at the Army Threat Systems Management Office (TSMO) as a member of the Threat Computer Network Operations Team (TCNOT). I provided key Computer Network Operations (CNO) support by performing validated threat CNO penetration testing and systems security analysis. TCNOT is the highest

level of implementation of the CNO Team concept.

5. From 2008 to 2017, I also worked through a professional staffing company for several testing laboratories that tested electronic voting machines. These laboratories included Wyle Laboratories, which later turned into National Technical Systems (NTS) and Pro V&V. My duties were to perform security tests on vendor voting systems for the certification of those systems by either the Election Assistance Commission (EAC), or to a state's specific Secretary of State's requirements.

6. I have provided consultation and technical analysis on several Georgia election complaints and inquiries. In that effort I have reviewed voting system certification test reports, test plans, EAC relevant documents, and Georgia election laws and regulations.

7. While conducting analysis of several Dominion election databases, from various states, I obtained four Georgia county databases from the 2020 election. These databases had originally been obtained via Public Records Requests. The counties were Appling, Bibb, Jones, and Telfair.

8. The focus of that effort was to compare Arizona's election database to other Dominion databases in, Colorado, Georgia, Michigan, and Pennsylvania in preparation for my declaration to the U.S. Supreme Court. The scope of this effort was to further examine the Georgia databases.

EXECUTIVE SUMMARY

9. An ***egregious*** security violation has been discovered, relating to the cryptographic encryption keys utilized by the voting equipment provided and serviced by Dominion Voting Systems, Inc. ("Dominion"). Dominion placed these encryption keys on voting system election databases unprotected and in plain text in violation of EAC-certification requirements and its contract with the state of Georgia. Analysis of the four counties election databases (Appling, Bibb, Jones, and Telfair) confirmed this security violation.

10. The secret encryption key and x509 certificate used to encrypt, decrypt, the election data, and used for authentication when transferring files and communication are stored in plaintext, unprotected within the election database. Compounding this, the database is not

configured to standard security configurations used for a database dealing with sensitive information. These findings indicate that all cryptographic safeguards, designed to ensure the security and accuracy of election results and data, have been rendered meaningless.

11. Upon analysis and review of the four Georgia databases, each database contained simple and easy to guess passcodes, common or shared passwords were also discovered. One anomaly found was that the same exact security code was being utilized in other states during the same election period. The same password and/or security code for certain accounts are identical to the password or security code used in Maricopa County, AZ and Mesa County, CO.

12. Given my education, experience as a security professional and years of experience working with Voting System Testing Laboratories (VSTL), and the thorough analysis of the systems, processes, and the electronic records detailed above, the facts have led to the conclusion that the voters of Georgia should have no confidence that their votes have been accurately counted, if they were even counted at all.

DETAILED FINDINGS AND CONCLUSIONS

13. Dominion's Democracy Suite systems use a combination of a Rijndael Key, a Rijndael Vector, a Hash-based Message Authentication Code (HMAC) and a x509 security certificate to encrypt, decrypt and to authenticate data. The encryption key is considered a secret key and should be hidden and protected. All the components listed above (security processes) should be stored encrypted, especially if stored within a database. In the Democracy Suite systems, they are not. They are left unprotected and out in the open easy to find. See the figures for each county in **Exhibit A**.

14. The purpose of using encryption in election systems is to prevent unauthorized access to those systems and to prevent malicious alteration of election results. EAC-certification requirements mandate that these encryption keys must be kept secret from unauthorized access. With these items anyone could manipulate system configuration files causing the tabulators to not function properly. They could create or duplicate election data and make it look authentic. The possible attacks or manipulation of data are endless.

15. Furthermore, the plaintext storage of passwords and encryption keys on **any** information system, let alone a voting system, is an **egregious**, **inexcusable** violation of long-standing, **basic** cybersecurity best practices. It destroys any type of security the system wishes to implement. Windows log-in is the only authentication needed to access the unprotected database where the keys are stored. Windows log-in can easily be bypassed.[1]

16. Electronic voting systems overall are full of vulnerabilities with multiple exploits available. The vulnerabilities range from outdated Operating Systems (OS), third party applications, to protocols and services. Adding to these weaknesses is system configuration. Nearly all aspects of the voting systems do not use standard security, let alone industry best practices when configuring their systems. Voting system vendors, like Dominion, lack basic configuration management of their systems.

17. The election database is a prime example of misconfiguration. It is standard practice for a database to not use OS authentication to access or modify the database. Democracy Suite versions use OS authentication, which increases the number of attack vectors on the database. Additionally, if a database is to hold sensitive data it should be configured to encrypt the table, column, or row to which the sensitive data is to reside. This prevents anyone with read only or unauthorized access from seeing the data.

18. These keys being plaintext outside of the cryptographic module also **violates** FIPS 140-2. Section 4.7 of FIPS 140-2 "Cryptographic Key Management"[2] states "The security requirements for cryptographic key management encompass the entire lifecycle of cryptographic keys[.]" The section also states that "Secret keys, private keys, and CSPs shall be protected within the cryptographic module from unauthorized disclosure, modification, and substitution." Section 4.7.5 "Key Storage" states "Plaintext secret and private keys shall not be accessible from outside the cryptographic module to unauthorized operators." Additionally, the National Institute of Standards and Technology NIST SP 800-57[3] section 4.7 "Key Information Storage" states "The integrity of all key information **shall** be protected; the confidentiality of secret and

[1] https://www.youtube.com/watch?v=2v-mGf4_9-A

[2] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf pg.30

[3] https://doi.org/10.6028/NIST.SP.800-57pt2r1

private keys and secret metadata **shall** be protected. When stored outside a cryptographic module[.]"

19. Georgia law requires that the voting system be certified by the EAC. O.C.G.A. § 21-2-300 (2022). The EAC requires voting systems to be tested for compliance with the Voluntary Voting Systems Guidelines (VVSG). The VVSG specifically include requirements for storing cryptographic encryption keys, expressly adopting the Federal Information Processing Standards (FIPS) defining the mandatory practices and management of these keys to include storage of the keys in a cryptographic module or to be encrypted themselves.[4]

20. Of note regarding the technical and supervisor passcodes, the string of numbers repetitively used as a passcode in the Georgia voting systems was also the same **exact** passcode found and used in both Maricopa County, Arizona and Mesa County, Colorado. This commonly known, easy to guess passcode, which was used across multiple states, increases the risk of possible exploitation exponentially.

21. Another anomaly like the one mentioned above also exists with some of the administrative account passwords and security codes. The Georgia accounts either share the same password, security code or both with Maricopa and Mesa County. See figures B-1 and B-2 in **Exhibit B**. The blue arrows on these figures highlight the out of state counties that have the same credentials. This is highly suspicious but more importantly it is a security concern.

22. I reviewed Dominion's response to these revelations.[5] Dominion's statement that "*The claim that access to any single credential could affect the result of an election undetected is implausible and conspiratorial*" is misleading for three reasons:

- While access to a "single credential" as characterized by Dominion, would likely not be sufficient to manipulate an election, that is not the situation here. The Dominion voting systems are so ill configured and full of vulnerabilities that one single user credential could gain access to the database where the encryption keys are left

[4] VVSG 1.0 (2005) 7.4.5.1 https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.0_Volume_1.PDF

[5] https://lawandcrime.com/supreme-court/kari-lake-to-scotus-hurry-up-the-2024-election-is-coming-and-dominion-voting-machines-need-to-be-banned/

unprotected and in plain text for the world to see.

- Access to these unprotected in plain text encryption keys provide the capability to unlock or manipulate other accounts.
- Lastly, the encryption keys provide the means with which to fabricate and/or manipulate election results, change the configuration of voting systems components such as the tabulator. Manipulation of election results could happen at any level; the tabulator, memory card, server, or database level, which would be accepted by the system as authenticated results.

23. Dominion's statement that "*Dominion's machines are fully certified by the U.S. Election Assistance Commission...*" is likewise misleading because EAC certification of a voting system is not strictly limited to its operation "as tested" and defined in the corresponding Scope of Conformance. EAC-certification is an operational standard which must be maintained within the specifications as defined in the VVSG throughout the use of the voting system. See, e.g., VVSG Sections 8.1 (discussing the conforming the system to meet VVSG and state and local requirements throughout the life of the system) and 9.5 (discussing establishment of procedures to resolve identified defects). Dominion's voting systems are not operating as tested and certified by the EAC.

24. Dominion is also not compliant with its contract with the state of Georgia for the reasons previously stated above concerning the encryption keys. Exhibit B to the Master Solution Purchase and Services Agreement Dominion states:

- Section 8. System Security Description "Dominion utilizes authentication and authorization protocols that meet EAC VVSG 2005 standards. In addition, Dominion's solution relies on industry-standard security features to ensure that the correct users based on a user role or group are granted the correct privileges."
- Section 8.3 Encryption configurations for both data at rest and data in motion "Data generated by the Democracy Suite platform is protected by the deployment of FIPS approved symmetric AES and asymmetric RSA encryption."
- Section 8.9 Secure Development Process "Data integrity and confidentiality is also

implemented according to NIST defined and FIPS validate procedures and algorithms."

None of these sections are being fulfilled with the voting system in its current state.

CONCLUSION

25. The analysis of the four Georgia county databases, the multitude of account and credential issues found, the numerous vulnerabilities associated with the voting system components leave the voting systems in Georgia lacking any system integrity. The encryption mechanisms and security certificates are left totally unprotected in a highly vulnerable system in violation of the VVSG and EAC certification requirements. The result of these critical faults, individually or collectively, means there is no way to know if votes cast in either 2020 or 2022 election were correctly recorded or tabulated. Also, as there is no evidence these issues and violations have been resolved, there is no way to know if the results for the 2024 election cycle will be correctly recorded or tabulated.

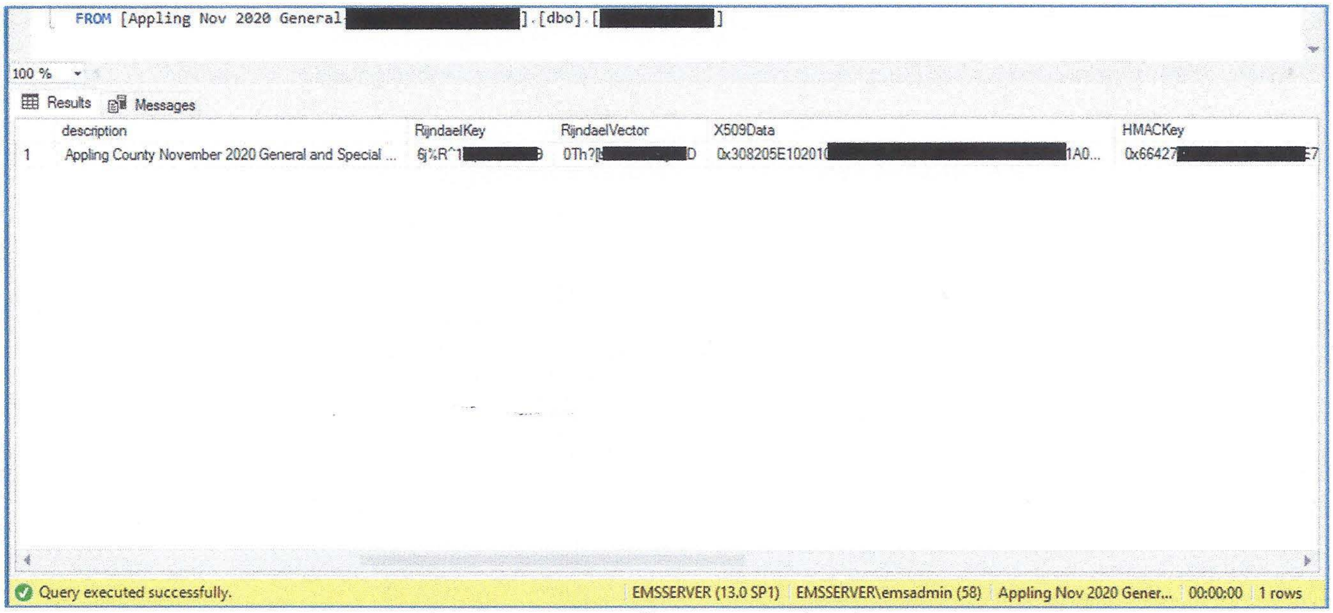
Sworn and subscribed to me
this 15 day of August 2024

Jacob Thorson Smith
Notary Public
My Commission Expires: My Commission Expires 05/21/2028

Clay U Parikh
Clay U. Parikh

JACOB THORSON SMITH
NOTARY PUBLIC
ALABAMA STATE AT LARGE

Exhibit A



```
FROM [Appling Nov 2020 General[redacted]].[dbo].[[redacted]]
```

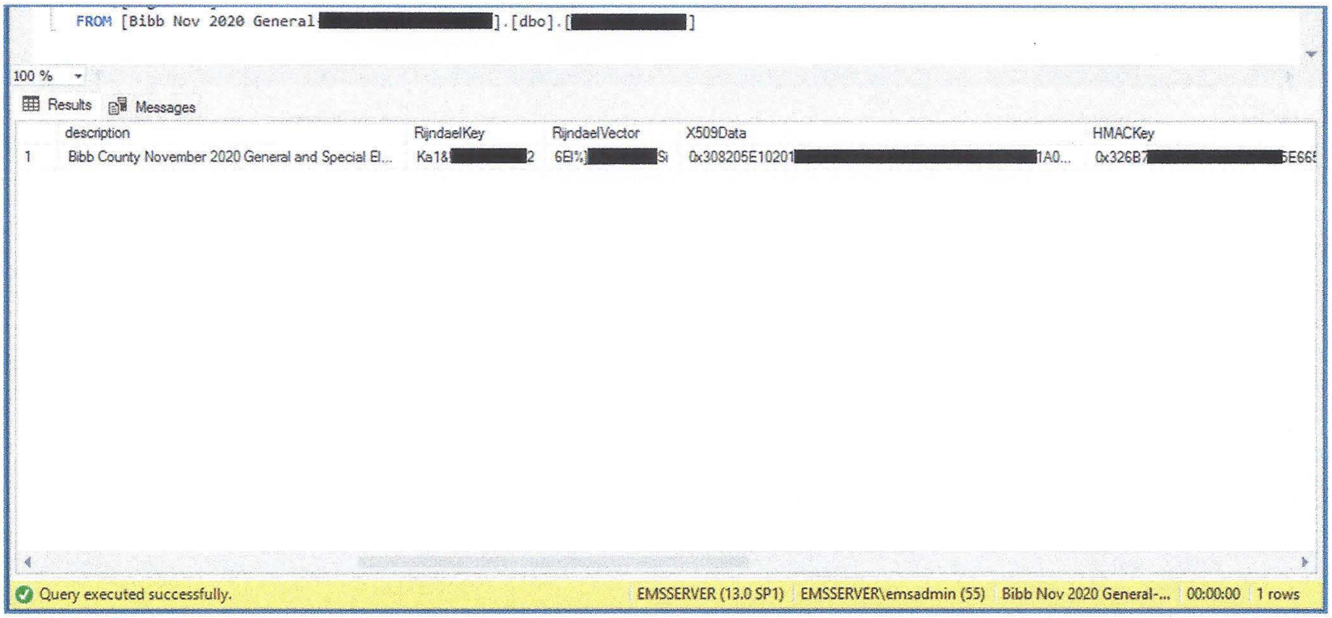
100 %

Results Messages

	description	RijndaelKey	RijndaelVector	X509Data	HMACKey
1	Appling County November 2020 General and Special ...	6j%R^1[redacted]9	0Th?[redacted]D	0x308205E10201[redacted]1A0...	0x66427[redacted]E7

Query executed successfully. | EMSSERVER (13.0 SP1) | EMSSERVER\emsadmin (58) | Appling Nov 2020 Gener... | 00:00:00 | 1 rows

Figure A-1. Appling encryption keys



```
FROM [Bibb Nov 2020 General[redacted]].[dbo].[[redacted]]
```

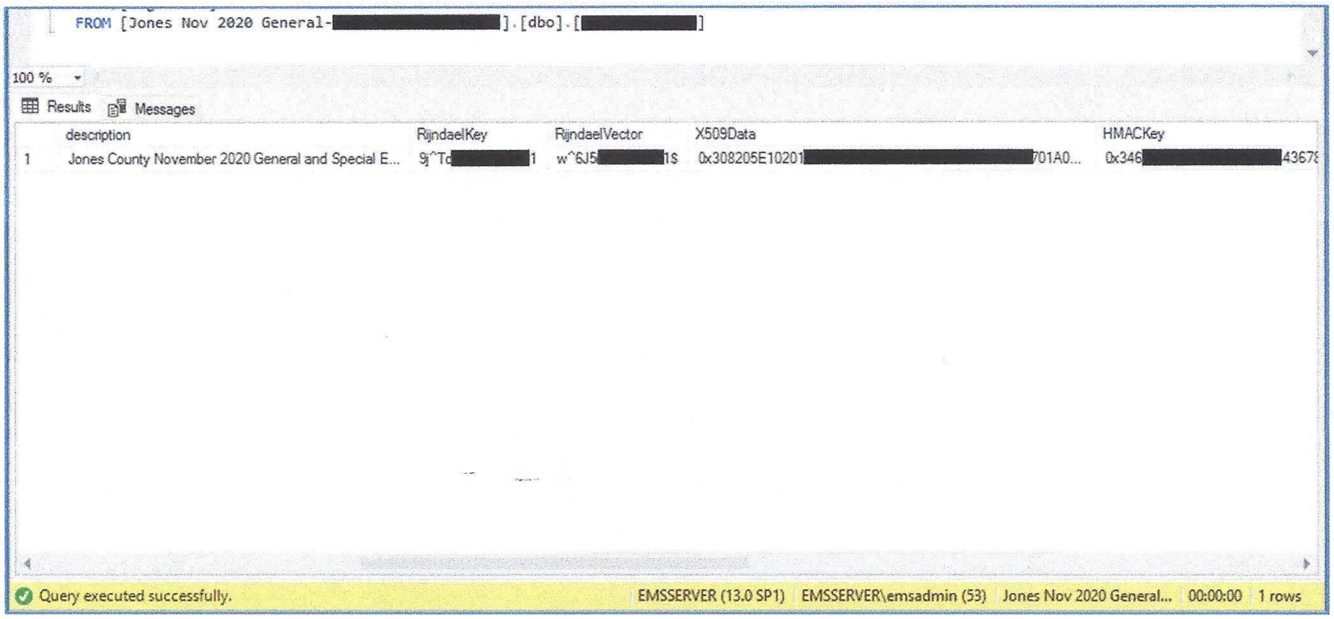
100 %

Results Messages

	description	RijndaelKey	RijndaelVector	X509Data	HMACKey
1	Bibb County November 2020 General and Special El...	Ka1&[redacted]2	6El%][redacted]Si	0x308205E10201[redacted]1A0...	0x326B7[redacted]5E665

Query executed successfully. | EMSSERVER (13.0 SP1) | EMSSERVER\emsadmin (55) | Bibb Nov 2020 General-... | 00:00:00 | 1 rows

Figure A-2. Bibb encryption keys

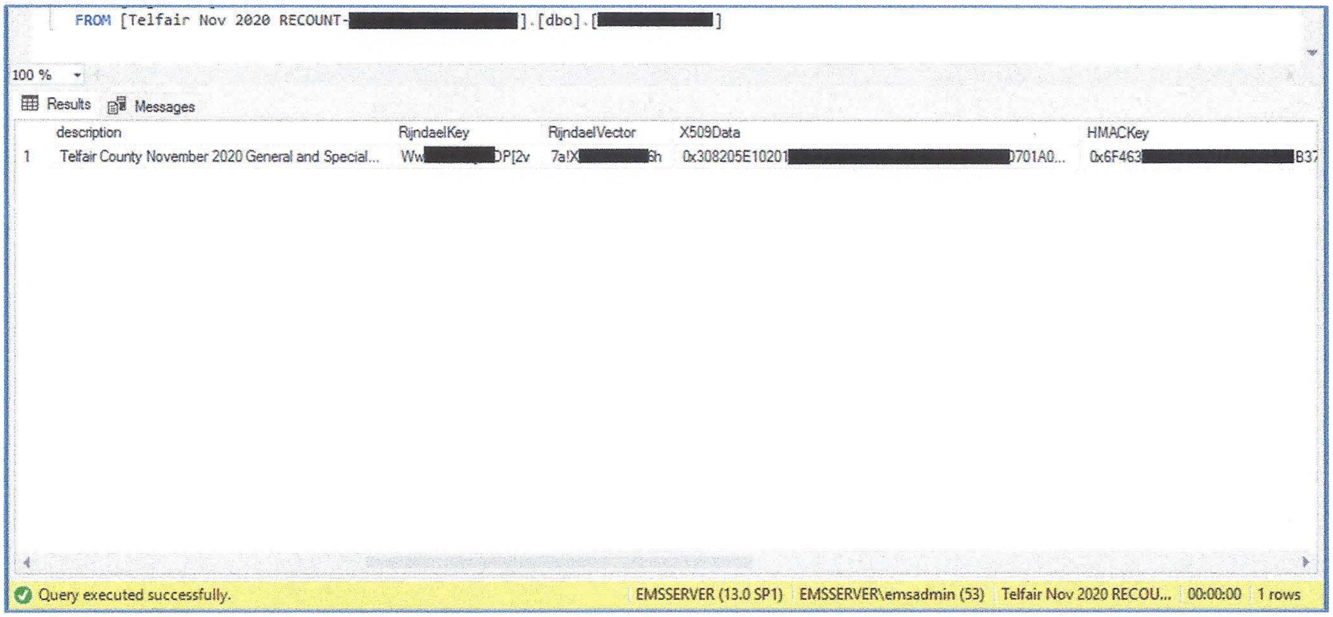


```
FROM [Jones Nov 2020 General-[redacted]].[dbo].[[redacted]]
```

	description	RijndaelKey	RijndaelVector	X509Data	HMACKey
1	Jones County November 2020 General and Special E...	9j^T[redacted]1	w^6J5[redacted]1$	0x308205E10201[redacted]701A0...	0x346[redacted]4367

Query executed successfully. | EMSSERVER (13.0 SP1) | EMSSERVER\emsadmin (53) | Jones Nov 2020 General... | 00:00:00 | 1 rows

Figure A-3. Jones encryption keys



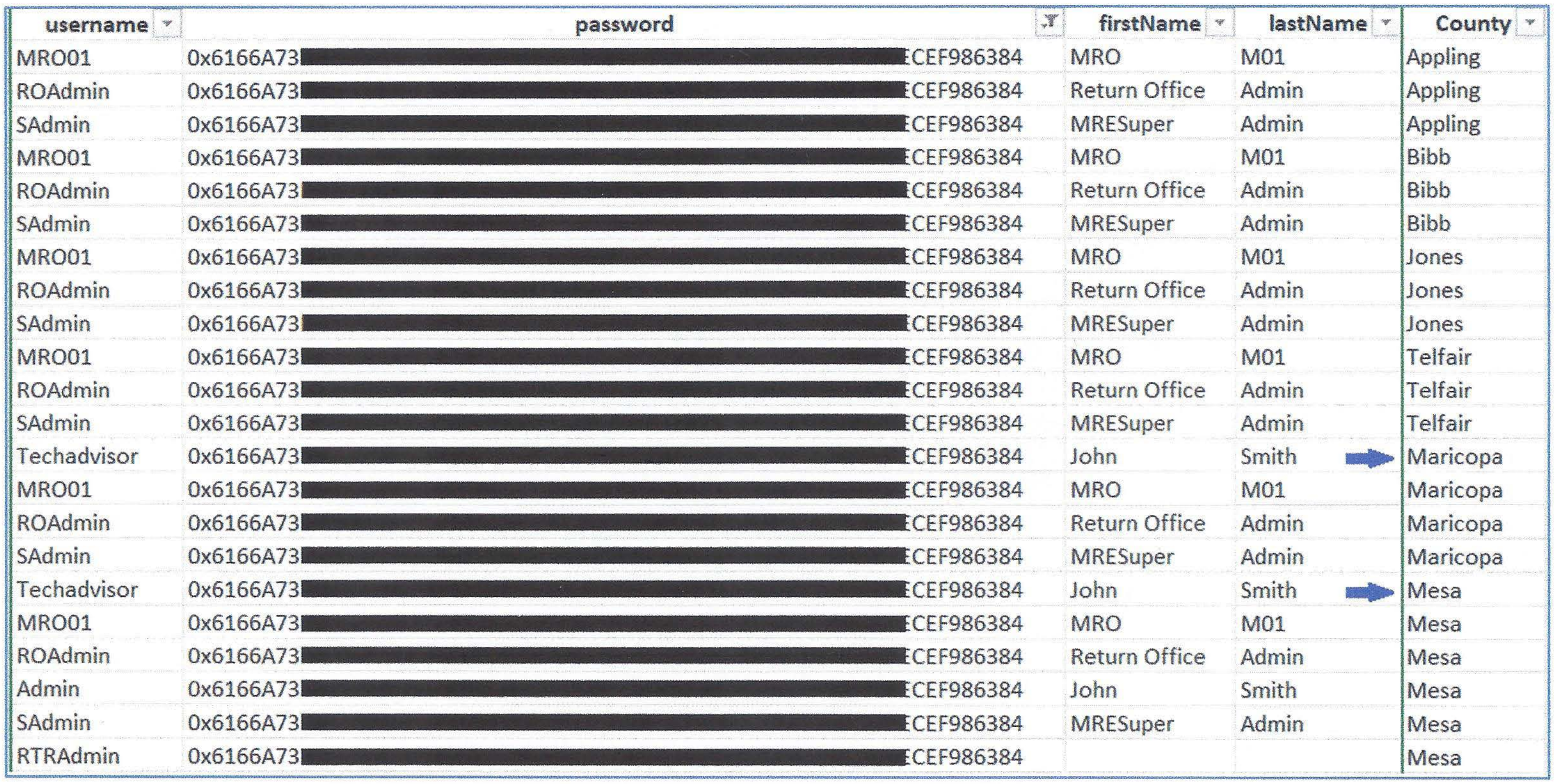
```
FROM [Telfair Nov 2020 RECOUNT-[redacted]].[dbo].[[redacted]]
```

	description	RijndaelKey	RijndaelVector	X509Data	HMACKey
1	Telfair County November 2020 General and Special...	Ww[redacted]DP[2v	7a!X[redacted]h	0x308205E10201[redacted]701A0...	0x6F463[redacted]B37

Query executed successfully. | EMSSERVER (13.0 SP1) | EMSSERVER\emsadmin (53) | Telfair Nov 2020 RECOU... | 00:00:00 | 1 rows

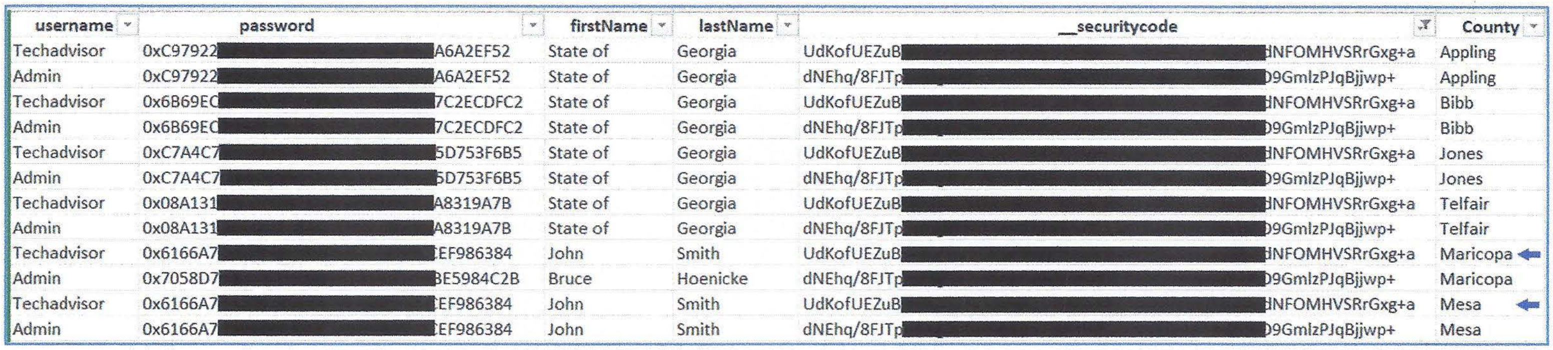
Figure A-4. Telfair encryption keys

Exhibit B



username	password	firstName	lastName	County
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Appling
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Appling
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Appling
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Bibb
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Bibb
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Bibb
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Jones
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Jones
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Jones
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Telfair
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Telfair
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Telfair
Techadvisor	0x6166A73[redacted]CEF986384	John	Smith →	Maricopa
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Maricopa
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Maricopa
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Maricopa
Techadvisor	0x6166A73[redacted]CEF986384	John	Smith →	Mesa
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Mesa
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Mesa
Admin	0x6166A73[redacted]CEF986384	John	Smith	Mesa
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Mesa
RTRAdmin	0x6166A73[redacted]CEF986384			Mesa

Figure B-1. Common Passwords



username	password	firstName	lastName	__securitycode	County
Techadvisor	0xC97922[redacted]A6A2EF52	State of	Georgia	UdKofUEZuB[redacted]NFOMHVSRrGxg+a	Appling
Admin	0xC97922[redacted]A6A2EF52	State of	Georgia	dNEhq/8FJTp[redacted]9GmlzPJqBjjwp+	Appling
Techadvisor	0x6B69EC[redacted]7C2ECDFC2	State of	Georgia	UdKofUEZuB[redacted]NFOMHVSRrGxg+a	Bibb
Admin	0x6B69EC[redacted]7C2ECDFC2	State of	Georgia	dNEhq/8FJTp[redacted]9GmlzPJqBjjwp+	Bibb
Techadvisor	0xC7A4C7[redacted]5D753F6B5	State of	Georgia	UdKofUEZuB[redacted]NFOMHVSRrGxg+a	Jones
Admin	0xC7A4C7[redacted]5D753F6B5	State of	Georgia	dNEhq/8FJTp[redacted]9GmlzPJqBjjwp+	Jones
Techadvisor	0x08A131[redacted]A8319A7B	State of	Georgia	UdKofUEZuB[redacted]NFOMHVSRrGxg+a	Telfair
Admin	0x08A131[redacted]A8319A7B	State of	Georgia	dNEhq/8FJTp[redacted]9GmlzPJqBjjwp+	Telfair
Techadvisor	0x6166A7[redacted]EF986384	John	Smith	UdKofUEZuB[redacted]NFOMHVSRrGxg+a	Maricopa ←
Admin	0x7058D7[redacted]BE5984C2B	Bruce	Hoenicke	dNEhq/8FJTp[redacted]9GmlzPJqBjjwp+	Maricopa
Techadvisor	0x6166A7[redacted]EF986384	John	Smith	UdKofUEZuB[redacted]NFOMHVSRrGxg+a	Mesa ←
Admin	0x6166A7[redacted]EF986384	John	Smith	dNEhq/8FJTp[redacted]9GmlzPJqBjjwp+	Mesa

Figure B-2. Common Security Codes

EXHIBIT B

Affidavit of Benjamin Cotton

EXHIBIT
4

Affidavit of Benjamin Cotton

1) I am over twenty-one (21) years of age, under no legal disability, and am otherwise competent to give this affidavit.

2) The matters sworn to herein are based on my personal knowledge.

3) I am the founder of CyFIR, LLC (CyFIR) and Cyber Technology Services, INC.

4) I have a Master's Degree in Information Technology Management from the University of Maryland University College. I have numerous technical certifications, including the Certified Information Systems Security Professional (CISSP), Microsoft Certified Professional (MCP), Network+, and Certified CyFIR Forensics and Incident Response Examiner.

5) I have over twenty-seven (27) years of experience performing computer forensics and other digital systems analysis.

6) I have over twenty (20) years of experience as an instructor of computer forensics and incident response. This experience includes thirteen (13) years of experience teaching students on the Guidance Software (now OpenText) EnCase Investigator and EnCase Enterprise software.

7) I have testified as an expert witness in state courts, federal courts and before the United States Congress.

8) I regularly lead engagements involving digital forensics, cyber security, and incident response for law firms, corporations, and government agencies and am experienced with the digital acquisition of evidence under the Federal Rules of Evidence.

9) In the course of my duties, I have forensically examined Dominion Voting Systems (DVS) components in Maricopa County Arizona, Antrim County Michigan, Fulton County Pennsylvania,

Coffee County Georgia, Mesa County Colorado. These system components are hereinafter referred to as the "Analyzed Election County Components".

10) In the course of my duties I have examined Dominion voting databases from the 2020 elections produced pursuant to public records requests from Appling County, Bibb County, Jones County, and Telfair County. These counties are located in the State of Georgia, hereinafter referred to as the "Analyzed Election Databases".

11) In the course of my duties, I have reviewed the administrative manuals and documentation for the DVS Democracy Suite software and hardware components.

12) In the course of my duties, I have reviewed the public information from the Election Assistance Commission ("EAC") and its certification process for election software.

13) In the course of my duties I have reviewed the report dated 1 July 2021 by Alex J. Halderman titled "Security Analysis of Georgia's ImageCast X Ballot Marking Devices".

EXECUTIVE SUMMARY

14) I performed a thorough analysis of the Analyzed Election County Components and Analyzed Election Databases and have determined that the encryption keys used to secure the results, encrypt and decrypt the tabulator results and protect the integrity of the EMS operations are stored in plain text in an unencrypted SQL database that is accessible with a simple SQL query. This egregious security lapse provides anyone with access to the voting system with the tools to alter election results without likely detection.

15) The State of Georgia knew about critical vulnerabilities in the ability of the Dominion Voting Systems to secure the encryption keys vital to ensuring the integrity of Georgia's elections in July of 2021 and have failed to address any of the vulnerabilities.

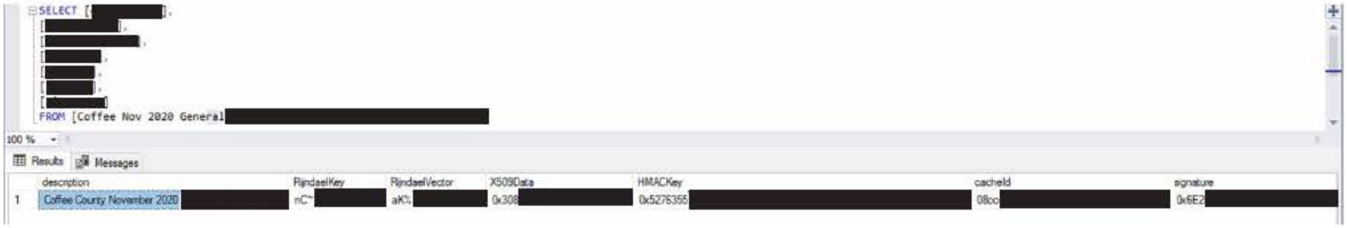
16) The Coffee County EMS has a compiler installed that provides the ability to modify and create executable files and drivers on the fly that could be used to alter election results without

detection. There is evidence that executable files were created and modified after the Dominion Voting Software (DVS) was installed and certified.

DETAILED FINDINGS

Unprotected Encryption Keys

17) In the course of my analysis, I determined that there was a flagrant failure to protect the election encryption and decryption keys within the election databases in the Analyzed County Election Components. The DVS Democracy Suite utilizes a combination of a Rijndael Key, a Rijndael Vector, a Hash-based Message Authentication Code (HMAC) and a x509 security certificate to encrypt, decrypt and authenticate data. This data includes code signing, data signing, communications, and tabulator results from ICC or ICP2 components. The protection of election encryption and decryption keys is prominently described by DVS within Democracy Suite Technical Data Package documents as the mitigation for the risk of a malicious actor tampering with the election database, election result files, scanned ballot images, device audit logs, device log reports, ballot definitions and other critical elements that could allow authorized or unauthorized parties, to alter the outcome of an election without detection. These keys have been left unprotected on the election database and are in plain text as shown below:



```
SELECT [[redacted]],
      [[redacted]],
      [[redacted]],
      [[redacted]],
      [[redacted]],
      [[redacted]],
      [[redacted]]
  FROM [Coffee Nov 2020 General[redacted]
```

	description	RijndaelKey	RijndaelVector	X509Data	HMACKey	cacheId	signature
1	Coffee County November 2020 [redacted]	nC~[redacted]	aK%[redacted]	0x308[redacted]	0x5276355[redacted]	08cc[redacted]	0x6E2[redacted]

Figure 1 - Rijndael Key for Coffee County GA 2020 Election

18) The only barrier to access these keys is the Windows-log-in. Given the egregious lack of current cyber security precautions on the Analyzed Election Components, this log in obviously would not prevent a malicious actor from changing results. An actor could easily bypass the

Windows log-in feature in about 5 minutes with well-known hacking techniques available on the internet. Given the cyber security vulnerabilities, including the sharing of passwords between user accounts, access to all of these encryption elements is easily obtained. The encryption elements are stored in the MS SQL election database and are easily retrieved with a simple SQL query.

19) 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. Anyone with local or remote access to the system, including authorized or unauthorized users, can obtain the certificates and keys and once obtained the entire election can be compromised. A simple example of the exploitation of these keys would be the modification of the results and .dvd files that are transmitted or copied from the ICC scanners, HiPro scanners and the ICP2 tabulators prior to the ingestion of these files into the EMS for counting. By leveraging the decryption/encryption keys it is possible to script a program that would automatically change the contents of the ICP2 tabulator .dvd files, results.txt and cast vote records files prior to ingestion into the EMS. This altered vote count would not be logged as an intrusion or an error. Simply put, it would not be detected on the EMS. As long as these keys are exposed and unprotected, the results of any election conducted on these systems can not be guaranteed.

20) It is clear from my review of the Alex J. Halderman report dated 1 July 2021 and titled ""Security Analysis of Georgia's ImageCast X Ballot Marking Devices" that the state of Georgia knew about the lack of protections of the encryption keys in the DVS ImageCast. Sections 6.1 and 6.2 detail in depth how to extract the keys from the cards used to authenticate to the ImageCast X (ICX) and acknowledges that access to these keys allows the changing of critical voting files including election results. There is no indication that these critical weaknesses in voting system security have been addressed.

The Georgia Voting Systems Contain the Ability to Modify and Create Executable Files and Drivers on the Fly

21) In computing, a compiler is a computer program that translates computer code, such as source code, to create an executable program that a computer can ‘run’. These executable programs can be the common filename.exe format, but also include device drivers with the .dll extension as well as other forms of lower level executable code. In order to ensure that no erroneous code is present on voting systems, the Election Assistance Commission (EAC) establishes a ‘scope of conformance’ that contains a list of the hashes for the Dominion Voting System software that undergoes the certification process. This is to ensure that no executable program or device driver is later created or modified. Changing or modifying the executable programs and device drivers should invalidate the EAC certification and decertify the system, but more importantly could change the expected behaviors of the system, be used to create malicious programs on the system, create or open external communications, or modify election results. In order to create or modify an executable file or driver the programmer must use a compiler. Analysis of the Coffee County Election Management System (EMS) determined that it contained eight (8) different versions of the Microsoft compiler named MSbuild.exe. These compilers were present on the system at the time of the 2020 election and are present now[1]. The MD5 hash values for these eight different compilers are 3b2790718535d05f209a542d05575dda, 3c03b4467059c385b175aeaacc228391, 88144380e37cea1e1fd2aee3568bb27e, 88de8fbbd91803eef67064b39d702650, 8dbf81c4ad4a899790bd325bed966aff, 913f5dbfb11f4d590670821e4da28c2b, 9e40eeeb04222dfa5f2f43f39b171ba3, and fc6370d7bd71895b795da0fb75c26985. None of these compilers are contained in the EAC Scope of Conformance.

[1] There is no public acknowledgement or announcement that any modifications or updates have been made to the Dominion Democracy Suite 5.5A acquired by Georgia and used in the 2020 elections.

22) Analysis of the Coffee County EMS further determined that one thousand nine hundred ninety one (1,991) executable files were created after the installation of the Dominion Voting System on 9/12/2019. One thousand one hundred seven (1,107) executable files were modified after the installation of the Dominion Voting System on 9/12/2019. None of these hash values for the executable files created or modified after 9/12/2019 are contained in the EAC Scope of Conformance for the certification of the Dominion 5.5A voting system. Had there been any effective monitoring of the files on the accredited system, this system should have been decertified for use in elections.

23) I have had the opportunity to examine Dominion Voting Systems in Arizona, Georgia, Michigan and Pennsylvania. The MSBuild.exe compiler has been present in all the examined systems. It is reasonable to believe that the MSBuild.exe compiler exists on all Georgia voting systems.

24) The current methodology of the EAC approved auditors is flawed in that it only checks for changes to a specific filename that is located in a specific file path. Based on my analysis the methodology does not check for new or modified executable files or drivers.

CONCLUSION

25) The presence of compilers on the system and placing the master cryptographic keys on the election database in plain text and unprotected allows any actor with access to the voting system complete control over the election results. Any changes to the voting results leveraging these keys would likely not be detected. This is an egregious breach of basic security practices that must be remedied immediately. No election results provided by these voting machines can be trusted given the subjects identified and described in this report. The fact that these vulnerabilities have not been addressed places the integrity and outcome of any election at risk.

SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 18th DAY OF AUGUST, 2024.

Benjamin R. Cotton

Sworn to and subscribed before me, this 18th day of August, 2024.

Notary Public
My commission expires: 9/29/27

KEANNA KRUEGER
COMMISSION EXPIRES
NOTARY
23037336
PUBLIC
9-29-27
STATE OF WASHINGTON

State of Washington
County of Kittitas
Signed and sworn to (or affirmed) before me on 8/18/24 by Keanna Krueger

Notary Public

EXHIBIT C

Hearing Transcript on Mandamus NISI
Before Judge Scott McAfee

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DEKALB COUNTY REPUBLICAN PARTY, INC.,)
)
Applicant,)
) CIVIL ACTION FILE
vs.)
) NO. 24CV011028
BRAD RAFFENSPERGER, IN HIS OFFICIAL CAPACITY AS THE SECRETARY OF STATE OF THE STATE OF GEORGIA,)
)
Respondent.)

ORIGINAL

HEARING ON MANDAMUS NISI BEFORE JUDGE SCOTT McAFEE

SEPTEMBER 30, 2024

9:00 A.M.

Fulton County Courthouse
136 Pryor Street, 5th Floor
Atlanta, Georgia 30303

****

Whitney S. Guynes, CCR
WSG REPORTING, LLC
3430 Heartwood Lane
Atlanta, Georgia 30340
(678) 770-3151
office@WSGreporting.com

APPEARANCES

On behalf of the Applicant:

HARRY W. MacDOUGALD, ESQ
Caldwell, Carlson, Elliott & DeLoach, LLP
6 Concourse Parkway
Suite 2400
Atlanta, Georgia 30328
(404) 843-1956 (T)
email: hmacdougald@ccedlaw.com

TODD A. HARDING, ESQ.
Harding Law Firm, LLC
113 East Solomon Street
Griffin, Georgia 30223
(770) 229-4578 (T)
email: kamikazehitman@comcast.net

KURT OLSEN, ESQ.
Olsen Law, P.C.
1250 Connecticut Avenue, N.W.
Suite 700
Washington DC 20036
(202) 408-7025 (T)

On behalf of the Respondent:

BRYAN P. TYSON, ESQ.
The Election Law Group
1600 Parkwood Circle
Suite 200
Atlanta, Georgia 30339
(678) 336-7249 (T)
email: btyson@theelectionlawyers.com

BETH YOUNG, ESQ.
ALEXANDRA NOONAN, ESQ.
Assistant Attorney General
Office of the Attorney General
Georgia Department of Law
40 Capitol Square SW
Atlanta, Georgia 30334
(404) 657-9932 (T)
email: eyoung@law.ga.gov

INDEX TO EXAMINATION

WITNESS:

* * *

INDEX TO EXHIBITS

* * *

PROCEEDINGS

September 30, 2024
9:03 a.m.

THE COURT: All right. Let's go on the record then. We've got 24CV011028, DeKalb County Republican Party, Incorporated, Applicant vs. Brad Raffensperger as Secretary of State.

If we could have parties and counsel identify themselves for the record.

MR. MacDOUGALD: Harry MacDougald, Kurt Olsen and Todd Harding for the applicant, the DeKalb County Republican Party, Inc.

THE COURT: All right. Thank you, Mr. MacDougald.

Good morning. And on behalf of the Secretary of State?

MS. YOUNG: Morning. Beth Young and Bryan Tyson on behalf of the Secretary of State.

THE COURT: All right. Welcome everybody. We'll start with a little bit of housekeeping.

Are the parties in agreement on takedown? Obviously, we did not provide for madam court reporter, and I assume there's been some arrangement. I just want to make that part of the record.

MR. MacDOUGALD: We haven't discussed sharing the takedown, so I'll ask if y'all would like to do that.

MS. YOUNG: Sure. We will.

MR. MacDOUGALD: Okay.

THE COURT: There you have it.

COURT REPORTER: Thank you.

THE COURT: I have received and reviewed all the pleadings we've had over the weekend and as are part of the docket, and we can set aside some time this morning to talk through some of the motion to dismiss arguments, and we'll do that in just a minute here.

I'll note I also -- we filed an order accepting the amicus brief filed on behalf of Cherokee County late last night, and I reviewed that as well, so just an FYI to the parties.

In dealing with the logistics, let me start out here and ask and inquire:
Mr. MacDougald, I think your initial time estimate was four to five witnesses, about four to five hours, including cross and that sort of thing.

Is that still your anticipation?

MR. MacDOUGALD: I think it's going to be a little bit longer than that. I've got a category of witnesses that I'm calling "authentication witnesses," and there are seven of those. I thought maybe it would be six; there's seven. They will be very short, each one of those. Three of them by Zoom -- one is elderly and two are in hurricane-stricken areas.

Then after those witnesses are finished, we will have two experts to testify. And I had guessed earlier that they would be two hours apiece, direct and cross. They might go a little bit more than that, but we'll just have to see.

THE COURT: All right. And those are the two -- the two expert witnesses, as you put it, I would assume are the heart of your case. Those are the ones you said that are here and you're hoping to have heard today?

MR. MacDOUGALD: Correct. It's Mr. Parikh and Mr. Cotton, and they're both from out of town.

THE COURT: All right. You had mentioned conferring with opposing counsel about whether there was a need for these authenticating witnesses. Anything come from those --

MR. MacDOUGALD: Actually, we haven't discussed that. I was just explaining what my plan was to them, but I don't think they have said what their position on that is, one way or the other. And what we're trying to authenticate are the back-up election databases from these four counties, and we have two approaches to that, Your Honor.

These items were produced to volunteers who made requests to the counties, that's four of the witnesses. They will say they got the flash drive, sent it up the chain -- and couple of hops, it make it to a website which was provided to them -- to Ms. McGowan, actually, in March.

Our experts downloaded the information from that side. There are hash files associated with these productions. That's an alternate or, you know, additional method of authentication, and the experts can talk about that, but they haven't had a chance to think about that or review that so I don't know that it's fair to ask them to --

THE COURT: I won't put them on the spot here. What I would ask, whenever we get an opportunity for a break here this morning, if you could provide to Ms. Young -- if she doesn't already have it -- the identity of these seven authenticating experts, exactly what you're trying to get in through them, and then maybe you can come back and you can tell me if you actually have a need for them.

MR. MacDOUGALD: All right.

THE COURT: I'd also propose that -- I don't necessarily know if we need them to be in that order. We can always start with your experts and we can prove it up later, I think, under 104(b).

MR. MacDOUGALD: That would work. And we do have a pro hac vice application for Mr. Olsen. It was submitted to the state bar. We don't have their response yet. I spoke to Ms. McGowan -- excuse me, Ms. Young about that just a moment ago, and she indicated they were not going to oppose the pro hac vice application for Mr. Olsen; so as a housekeeping matter, I wanted to bring that up.

THE COURT: Okay. Let's get to that in a

minute. Let me make sure I don't forget some other things.

MR. MacDOUGALD: Okay.

THE COURT: So in terms of the authenticating experts and using Zoom, any positions on that, Ms. Young?

MS. YOUNG: That's acceptable to us.

THE COURT: Okay. All right. And then when it comes to any conflicts and logistics, I know Ms. Young indicated she has quite an active week here in Fulton County, so we're going to accommodate those, we're going to work around those. My understanding was that there is a statutory imperative that we begin this in 30 days, but there's not necessarily -- the end date is not determined.

So we'll see as we make our way through it where we can -- if we need to pick up where we left off at some later date or perhaps we see how far we get today and go from there, but if it doesn't make sense to pick it back up Wednesday, maybe Thursday -- we'll find a different time.

All right. Other than the pro hac, was there any other thing we need to bring up before we get into the motion to dismiss on behalf of the -- let me start -- on behalf of the petitioner?

MR. MacDOUGALD: No, I think those are the housekeeping matters we needed to address.

THE COURT: Okay. Ms. Young, anything on behalf of the Secretary of State?

MS. YOUNG: No, Your Honor.

THE COURT: All right. No conflicts today? We've got you today?

MS. YOUNG: Yes.

THE COURT: Okay. So with the pro hac, Ms. Young, I looked at the application, any position on your behalf?

MS. YOUNG: We defer to the court on that, Your Honor.

THE COURT: Okay. Mr. MacDougald, what is the expected role of -- for Mr. Olsen in this proceeding?

MR. MacDOUGALD: I will be handling the witnesses and making the arguments, but he knows a lot about the case, and he's a good lawyer, and he's helping me, and so I would like to have him at the counsel table.

THE COURT: All right. So really the only request here is he's at counsel table with you and you're conferring with him; but otherwise you're making all the arguments, you're presenting the evidence, you're doing everything else?

MR. MacDOUGALD: Mr. Harding is going to step up to the plate on their motion in limine.

THE COURT: Okay.

MR. MacDOUGALD: There may come a time where it's necessary for one or the other of them to appear if there's a hearing in the -- between October 10th and 23rd. I have some international travel scheduled, and I don't --

THE COURT: I certainly think we're going to get this done before then.

MR. MacDOUGALD: I don't want that to delay the case, and if I have to, I'll appear by Zoom.

THE COURT: Okay. All right. Understood. Well, I'll say this, and then I can reduce this to a written order if there's a request, but if essentially Mr. Olsen's role is just here in an advisory capacity just sitting at counsel table, it will just be a conditional approval on those grounds.

MR. MacDOUGALD: Thank you very much, Your Honor.

THE COURT: All right. With that, then, let's move on to the motion to dismiss. Again, I've reviewed it. I've reviewed that and the response, and I anticipate taking it under advisement here this morning with the -- reserving the right to revisit it at any point during the evidence or at the conclusion of the case, but if we want to hear some preliminary arguments, I wanted to give each side 10 to 15 minutes to go through some of those. After any follow-up questions we can explore some of that.

So Ms. Young, your motion?

MS. YOUNG: Thank you, Your Honor.

With all due respect to the court's plan to take it under advisement, it's our position that the court need not even move into the evidentiary phase of this proceeding because it is so clear from the face of the application that this does not state a valid claim for a writ of mandamus.

A writ of mandamus is an extraordinary remedy, and is only to be granted when there is a clear legal right to the relief that it seeks.

There are two statutory provisions that the petitioner claims are at issue here, and there is really no factual dispute that the Secretary has complied with any legal duty that he has under either provision.

The first provision required the Secretary to purchase a system that was EAC certified. He did that. I don't think there's any dispute as to that. In fact, in their motion they don't take issue with the fact that it was, in fact, a certified system by the EAC, they just said, well, that can't possibly be the end of the requirement. They seek to impose some extra judicial -- or extra statutory, kind of, continuing certification requirement on the Secretary. That's not the way that it works, and there's no evidence or allegation in there that that's the way that it works.

The EAC certification is something that is given to a system. There's no yearly review or renewal or anything like that. If the legislature had wanted to impose some kind of an ongoing obligation on the Secretary or a third party to, you know, continuously update or monitor compliance with EAC standards, the legislature knew how to do that.

The second requirement they talk about is the Secretary's certification of the safety of the system. Again, the Secretary has done that. They don't take issue with that either. They just feel like the Secretary should not have done -- have given the certification in the way that he did. That goes to the heart of the discretionary duty, which is not an appropriate basis for a writ of mandamus.

You know, one way of illustrating this, I think, is to look at the unusual nature of this proceeding. A writ of mandamus is given an expedited tract for a reason. It should be very simple cases. You know, Official "X" had a duty to do "Y," and if you need an evidentiary presentation, it should be very brief. You know, you call a witness that says this official didn't do this thing. And if that is correct, the court says, Official "X," go do that thing. That's not this proceeding.

They are seeking to put on a full presentation of the same tired claims that have been rejected by courts all over the country again and again. The same claims that these plaintiffs are making have led to sanctions in other cases. Not just a finding of lack of merit, but sanctions against the parties and the attorneys. And if you look at the relief requested by the plaintiffs -- or petitioners I'm sorry -- again it's not mandamus relief. They want this court to order this and that, to have to go change this, and go get this certification here, and implement this new standard there -- that's not mandamus relief. Mandamus relief would be, you didn't certify, Mr. Secretary, that the system was safe. Go certify it. But the Secretary has already done that. If you look at the plain language of the statute, the instructions that were given by the General Assembly to the Secretary are clear, and they've been followed, and they've been followed appropriately.

Second of all, the timing of this action is particularly suspect. At the very latest, the petitioners knew about this in March, and --

THE COURT: So you mention that because of the e-mail. I think they push back and say, well, the actual applicant only found out in August. I don't quite remember where that is established. How -- so that's a factual dispute, right, when they found out from, I guess, their now counsel of record this certification issue?

MS. YOUNG: These are tired old claims that have been trotted all around the country. If the applicant wasn't --

THE COURT: How would you establish the petitioners' specific knowledge of them?

MS. YOUNG: Well, the applicant had a duty to go and seek reasonable knowledge if this is something that was concerning to them, and there's not much credibility in the claim that these petitioners didn't know or couldn't have known of this claim until right before the election.

THE COURT: Is that an issue of fact that perhaps a motion to dismiss is not going to be the right vehicle to make that argument?

MS. YOUNG: I think that given the amount of court proceedings that have been litigated over these same exact claims all over the country, I think the court could presume and infer knowledge to elections officials that the Dominion voting system has been challenged many,

many times in court and many, many times has been found to be safe and found to have not caused any material errors in elections.

Finally, the relief requested is really inappropriate here, because they can't ask for proper mandamus relief, because anything that they could ask for that would be proper has already been done. If you look at the plain language of the statutes, the Secretary has done exactly what has been required.

Now what they seek to do is, sort of, open this other door to what really is a different kind of case because, you know, one problem that they've had all over the country is getting dismissed on lack of standing. Now mandamus has very, very liberal standing requirements here in the state of Georgia. I'm sure that's why they filed a mandamus case. But just because they got their foot in the door doesn't mean they have a proper case and doesn't mean this court should entertain the type of a jury trial that is not appropriate on a mandamus action.

This court's focus should be limited to what is the specific statutory duty? Is it ministerial or discretionary? And is there even an allegation here that the Secretary has breached a clear, legal duty? There are some clear legal duties in the statute: Purchasing an EAC-certified system -- check, and certified that the system is safe -- check. Both of these things have been done. The petitioners are not going to be able to offer any evidence to the contrary and have done everything short of stipulate to that, and because of that, we don't think that this complaint states a claim for mandamus relief.

And the last thing that I want to say, because I know that you're about to hear a whole lot of fear mongering about things like encryption keys, the Secretary of State has done a thorough and diligent job of exercising his discretion in terms of ensuring the security of the system.

I don't happen to understand computer systems very well, that's why I have Mr. Tyson here to help me out, but if you think about an encryption key like a hotel key, when you check into a hotel room, you know, you leave on Saturday, that key is coded to stop working, so the next person that checks in on Sunday can't use your key to get into the room, and that's the same situation we have here.

Yes, there were encryption keys found that were produced through an open records request, but just, sort of, the same way that if I left my hotel room key on the hotel bar, that doesn't mean you can do anything with it. The Secretary puts -- and the counties, actually, put the system through rigorous checks and balances. We've had risk limiting audits, logic and accuracy testing. New encryption keys are issued for each election, so those encryption keys, just like hotel room key, aren't going to do anything for this election.

For the things to happen that they are talking about you'd have to have not just physical access to the machine, but because they are not connected to the internet or to other precincts, you'd have to basically engage in a kind of mission-impossible-level operation that would require a whole lot of Tom Cruises to pull it off. You'd have to have people with pins and USB codes and really good slight of hand to do all of this unnoticed by all the poll watchers that are there, the election workers that are there in these precincts.

So I would ask as you listen to what I know that they're going to talk to you about that you keep in mind that there are more layers of safety there than just the machine's software all by themselves. You've got a robust level of physical security that operates on top of that.

So to the extent that they claim that there is a vulnerability, they can't make the claim that this vulnerability has ever been exploited or ever will be exploited. And I say all that because I think it's important, given that I know that they're going to talk about it, that doesn't mean that this court should entertain it. This is a mandamus case. This is not any other kind of case. And this court's focus needs to be on just what the clear legal duty is, and the Secretary has done his duties under the statute.

Thank you.

THE COURT: Well, Ms. Young, one last thing I wanted to ask you about was, kind of, in the mandamus procedural hurdles to clear here, you say there's an adequate legal remedy here. Have you ever seen this presented at the appellate level of a post-election challenge being a sufficient cure for things that could come up beforehand? Is having to redo an election really an adequate remedy if the first one was bungled in some way?

MS. YOUNG: Well, we would start from the standpoint that there's no evidence that there will be a risk of a bungled election. But, yes, there have been cases where if there is some kind of a problem with an election, there have been times that courts have, you know, in certain precincts or in certain areas have ordered things like recounts.

And there is a really robust procedure before you even get to the point of an election contest where if there is, you know, something going wrong, say, at a precinct with some voting machines, for the workers at that point to come in and figure out what to do to correct for it. If they need to do a hand recount because the machines went down, they can do that before you even get to that point; so if all of the safeguards --

THE COURT: That's been applied in, like, a mandamus or an injunctive posture well before the election -- have we ever seen that, kind of, definitively-stated -- we won't address this here, because you have an adequate remedy come election day?

MS. YOUNG: That is commonly found in cases where there is no present danger of -- I can't think of one off the top of my head, but I could probably find you one, you know, when I sit down.

But certainly, you know -- first of all, there is case law that, you know, says that you assume that public officials are going to operate in good faith, and there's no evidence to the contrary here, from the Secretary on down to the poll workers that check you in when you get there to vote. We presume in the absence of evidence to the contrary that everybody in the system is going to act in good faith. And the safeguards that the system has, both in itself and operating all around it, physically, you know, at the polls are sufficient safeguards for the Secretary to have been able to, then and continuing to today, to certify that the system is safe and secure.

The statutory requirements have been met, and there's nothing to mandamus here. There is nothing for the court to tell the Secretary, go meet your statutory duty.

THE COURT: All right. Thank you, Ms. Young.

MR. MacDOUGALD: Good morning, Your Honor.

THE COURT: Good morning, Mr. MacDougald.

MR. MacDOUGALD: So before taking up the motion to dismiss, I would like to just give the court a thumbnail of what the case is about as we see it, action for mandamus. We seek an order compelling the Secretary to comply with his legal duty to field an election system that complies with the requirements for certification by the U.S. Election Assistance Commission, or EAC. The statutory source of that duty is 21-2-300, which provides for EAC certification, and Counsel is correct, there is an EAC certification.

And by the way, Your Honor, before I forget, I have an exhibit binder, which I would like to hand up, and then we'll have one for the witness, as well, but that's for the court's convenience.

We have the actual certification as part of our exhibits. The certification requirements under the EAC require compliance with something called the Voluntarily Voting System Guidelines. So in the context of certification they're not actual voluntarily. The system has to comply. That's not disputed.

The VVSG, Voluntarily Voting System Guidelines, impose cybersecurity requirements, and among those is compliance with a federal cybersecurity standard called FIPS 140-2, which is Federal Information Protection [sic] Standards 140-2. So the entire set of obligations imposed by the statute is certification, VVSG compliance, FIPS 140-2 compliance.

And our application alleges, supported by expert affidavits, that the election system in Georgia does not, in fact, comply with those standards notwithstanding the pre-purchase certificate, and it does not comply with respect to the storage and management of encryption keys.

Well, what the heck are encryption keys? It's a cipher, or a key, that's used to encrypt or decrypt information, and you may remember that the Enigma system used by the Germans in World War II, once they obtained the key, they were able to read all of the messages. They're used ubiquitously on computer systems for the transmission, processing, storage of information. When you do online banking it relies on encryption keys.

The standards require that those keys be kept safely and securely. On Georgia's election systems they are not. The FIPS 140-2 standard requires they be kept in what's called a cryptographic module. In fact, in the election databases they're stored in plain text, unencrypted themselves in plain text in the election database, and that's the case on all election servers and systems that have been examined by our experts, not just in Georgia but in other jurisdictions made by the same manufacturer.

We allege, and our experts say, that that is grossly non-compliant with the requirements of EAC certification, which means it does not comply with the statute.

THE COURT: And your petition, the sole statutory provision we're concerned with is

21-2-300, right? There's no greater universe?

MR. MacDOUGALD: Correct, (a)(2) and (a)(3).

THE COURT: All right. And so -- and I think the heart of your case is that this is an ongoing duty.

MR. MacDOUGALD: Correct.

THE COURT: And so, if this is a matter of plain language of this statute, what would you point me to to say that that is plain and unambiguous, and how do you account for the seemingly temporal confinement of "prior to" in paragraph (a)(3)?

MR. MacDOUGALD: Okay. So there's two things to say about that, Your Honor. One is that the pre-purchase certification requirements, (a)(2), there's a second certification that's required under (a)(3) where the Secretary, himself, makes the certification -- excuse me, I've got them reversed. (a)(3) is the EAC, and (a)(2) is the Secretary's certification that the system is safe and practicable for use, and that means in their actual operational use in elections. It can't mean anything else. It doesn't say safe and practicable for testing, it says safe and practicable for use.

The other -- the rest of the argument is to apply rules of statutory interpretation to the EAC certification requirement. And if it is read as the Secretary's counsel argues, it would be a meaningless gesture, security theater, if it is only required to be compliant in the testing environment and not the operational environment. And statutes are construed so that the -- you know, we presume the legislature does intend futile or useless gestures just for show. It intends that the system be secure in use -- safe -- safe and practicable for use.

It would be absurd to say that he has completed his duty as the chief elections officer in Georgia to oversee the purity and regularity of elections that all he's got to do is get a certificate before it's ever used and that when it comes to his attention emphatically that it is not, that he can do nothing. And the evidence will show, and we allege in our application, that the Secretary was first made aware of the encryption keys' vulnerability in July of 2021 when the plaintiffs in the Curling litigation delivered the Halderman report, it's called.

THE COURT: You talk about that in the brief.

MR. MacDOUGALD: Yeah.

THE COURT: This might be a tangent here, but I'm going to chase after it for a minute. I noticed that this is going to be amended, it's going to change effective January 1, 2025, the statute we're talking about?

MR. MacDOUGALD: Right.

THE COURT: Are any of these provisions at issue that were at the heart of your petition changing as a result? Maybe that also can be used as an indicator of statutory intent.

MR. MacDOUGALD: To be honest with you, I haven't looked at that and I don't know the answer.

THE COURT: We can cure that.

MR. MacDOUGALD: Yeah. I apologize.

THE COURT: I'm going to ask about your gross laches argument.

MR. MacDOUGALD: Sure.

THE COURT: I'm wondering -- you cite Justice Lumpkin from 1848.

MR. MacDOUGALD: Yes.

THE COURT: I'm wondering if we've had any other, maybe, cases addressing laches since then --

MR. MacDOUGALD: Yes, yes.

THE COURT: -- that talk about more -- I guess there's a decade delay. Have we seen others applied in the context of months or, kind of, case specific?

MR. MacDOUGALD: Well, nothing in this factual context that I was able to find.

THE COURT: Maybe not so much the election context, but maybe something that was a little more time sensitive.

MR. MacDOUGALD: Right. So there was a case that we cited in the brief called Marsh vs -- I can't remember who the defendant in the Marsh case was.

THE COURT: That one, I think, just kind of clarified what the standard was. It didn't really, as I recall, say a time frame is appropriate here.

MR. MacDOUGALD: Right, right.

There is a case cited in Marsh -- I think it's in our brief -- the plaintiff sued the

Commissioner of Roads and Revenues for DeKalb County. The plaintiff was the lessee on a lease for an airport. The Commissioner was required by statute to record the lease -- did not do it, and didn't do it for 16 years. And then the plaintiff, who did not know that it had not been recorded, and was entitled to rely on the presumption that the public officer performs their duty properly, brought the mandamus after 16 years.

THE COURT: So that case seems to hinge more on the knowledge aspect.

MR. MacDOUGALD: Correct.

THE COURT: I understand. I'm wondering more if you found any that, kind of, set a floor or a ceiling on -- you have knowledge, and here's how long you waited.

Have you found anything on that?

MR. MacDOUGALD: No, not definitive parameters on that, and I've been, you know, rolling this around in my head -- what's the difference in gross negligence and regular negligence and laches and gross laches, and I think it boils down to more adjectives about how bad it is, but doesn't really illuminate a clear parameter.

THE COURT: And what happened in August that -- right when you claim that --

MR. MacDOUGALD: Yeah. Our client, DeKalb County Republican Party, the chair, Marci McCarthy is here, and she can testify about this, but -- and this is not in the complaint. I mean, there's nothing in the allegations that would support a finding of laches on the part of the DeKalb County GOP, but the testimony will be that she learned about the encryption keys issue in July of this year, and this case was filed in August.

Now, you know, you can say, well, the Halderman report was made public in July of 2023, but, you know, what does that prove? The Halderman report -- that's not that long ago, and the Halderman report does not speak of certification requirements. It only speaks of the encryption key vulnerability itself and describes it as a very alarming and serious cyber vulnerability. Now that's a very long report, but it's in there, and it's in two places, Section 6.1 and Section 9.

And the -- so it was on the table, it's

been on the table with the Secretary ever since then, but they haven't done anything. In March of this year --

THE COURT: You're kind of putting that knowledge requirement on the Secretary, but with laches it's understood that the sole focus is on DeKalb.

MR. MacDOUGALD: Right. So there's not going to be any evidence that the DeKalb County GOP has slept on its rights.

And, you know, what Mr. Olsen knew and when he knew it is a different thing. You know, before he is engaged to represent, his knowledge is not attributable to the plaintiff. Now, the argument was made that these are tired, old claims. They've been adjudicated, been found without merit. There's been no adjudication on the merits anywhere in the United States on the encryption keys issue, nor the certification issue as it relates to the encryption keys.

And Exhibit 5 to the application is e-mail correspondence between Mr. Olsen and Ms. McGowan where he brings it to her attention, gives her an affidavit from Mr. Parikh -- that was in March of this year, offered to help the

Secretary address the problem. No response.

So there is not going to be any evidence of laches nor any evidence of gross laches, and if they're -- it's a factual question, anyway, as you alluded to anyway during Counsel's argument.

THE COURT: All right. Last question I have for you, just kind of getting back towards the, kind of, traditional tools we use to glean meaning from statutes if there is ambiguity or even just to confirm what we think the plain language says. You know, we'll see if maybe the revisions have any effect on that, but are there other similar provisions or is there anything else somewhere, elsewhere in the code, that you think is also going to shed light on this particular provision or are we just solely within the sections of 300?

MR. MacDOUGALD: Well, the only other code section that I would invoke is the code section on statutory interpretation about what is the evil to be corrected, you know, seek all [unintelligible] to fulfill the legislative purpose, and it would attribute to the legislature a futile gesture to merely require -- and there's one other point I'd like to bring up on this continuing obligation. The VVSG, itself, which is incorporated into the statutory requirement imposes a continuing compliance obligation.

THE COURT: Sure. I think you laid that out in your petition.

MR. MacDOUGALD: Okay.

THE COURT: But when you talk about the reference to legislative purpose, which is just another way of saying intent, is that -- is there a preamble or some other thing related to this code section that we should know about or is that purpose solely to be gleaned from that one code section?

MR. MacDOUGALD: Well, you know, Robert Bork said that when you're searching the legislative history for legislative intent, the judge is the one that packs the bag himself, so it's a little bit hazardous to stray beyond the text. But when this system was being considered by the legislature, and before it was being considered by the legislature, there was a commission created by the Secretary of State to examine the different vendors' systems and evaluate them for cybersecurity.

So any time there's a discussion of computerized election machines, cybersecurity is a top-of-mind concern. So we can infer that the legislature required EA [sic] certification in order to meet the public need of having a secure election system. And the contract with Dominion requires continuous compliance with cybersecurity standards.

THE COURT: The requirement for the Secretary of State to enter a contract, that's not a requirement of statute?

MR. MacDOUGALD: No, but it's -- the 21-2-300 (a)(3) speaks of purchase -- pre-purchase, so there's going to be a contract for purchase, and the EAC certification is a term and condition that the vendor has to meet before the Secretary can buy it. And the Secretary did buy it, and he -- and he bargained for and obtained contractual commitments to comply with all applicable standards, including federal information protection standards.

THE COURT: I mean, could the EAC -- hypothetically, and I'm not saying this is a good idea -- could the EAC just decide tomorrow, no more ongoing compliance that we require?

MR. MacDOUGALD: No. No, because the testing by the EAC on their website says that the systems are tested against the VVSG. The VVSG requires ongoing compliance, so they would be repudiating their own certification guidelines --

THE COURT: Federal guidelines.

MR. MacDOUGALD: -- if they took that position.

THE COURT: Okay. All right. Thank you, Mr. MacDougald.

MR. MacDOUGALD: All right. I guess you don't need to hear from me about the adequate remedy at law?

THE COURT: I feel like -- I think that was addressed in the brief.

MR. MacDOUGALD: Very well. Thank you very much.

THE COURT: So, as indicated, I'm going to reserve the ability to come back and make a ruling on these issues, and I want to give the petitioner the opportunity to present some evidence to make a record, and so I think we need to press onward here.

So -- and, as it relates to that, on the motion in limine to exclude both of these experts coming before the case, I think they play right into the same kind of arguments in terms of the relevance, the 403 objections.

Certainly, if the motion to dismiss arguments on the statutory intent are accepted, I think those would be on point, but since I'm deferring those, I think those would also, kind of, travel along with it. So the other issues in terms of the qualifications and whether they should be tendered as experts, I think that is something that we can handle through their testimony once they're on the stand and are likely to go to weight and not admissibility, so with that I think we can proceed, and Mr. MacDougald you can call your first witness.

MR. MacDOUGALD: I do have one more housekeeping matter. My two experts are in the courtroom, and I'd ask they be allowed to remain in the courtroom as experts to take in the testimony that's presented.

THE COURT: All right. Ms. Young?

MS. YOUNG: We would suggest that the rule of sequestration prevents that and would object to that. And they haven't been qualified as experts yet.

THE COURT: They have not; however, I would anticipate that they've testified -- I mean, I can't say I have their CV right in front of me, but they've testified as experts before, and --

MR. MacDOUGALD: Many times.

THE COURT: So I would anticipate they're likely to be allowed to testify on that behalf, and I don't think the rule of sequestration limits the number of experts that may sit in and review and hear each other's testimony.

Have you got anything more specific for me, Ms. Young, that makes it -- other than that initial bar of, hey, they may not be experts at all, is there anything else under the sequestration you think that keeps them out of the courtroom?

MS. YOUNG: I think we've expressed it in motion of limine and you've already ruled on that, so I don't want to belabor the point.

THE COURT: Okay. Fair enough.

I'll find -- the rule is invoked. If there are any other witnesses, especially those watching online, Mr. MacDougald, so I'd ask you to inform your seven other potential witnesses or maybe you alluded to --

MR. MacDOUGALD: I need you to excuse yourselves. If I have any other witnesses in the courtroom I need you to excuse yourself. Please step out. I haven't actually met all of them in person.

THE COURT: Well, that always bodes well.

MR. MacDOUGALD: It's a little hazardous, I will say.

THE COURT: All right. With that, you can call your first witness.

(Witness sworn.)

WHEREUPON:

MARCI MCCARTHY,

having been first duly sworn, was examined and testified as follows:

BAILIFF: Please state and spell your first and last name for the court.

THE WITNESS: My name is Marci McCarthy.

EXAMINATION

BY MR. MacDOUGALD:

Q Good morning, Ms. McCarthy.

How are you employed?

A I own a company called Tech Exec Networks, T.E.N. That is how I'm employed.

Q And how long have you been there?

A I have been there since 2010.

Q And what is the nature of that business?

A We are a cybersecurity marketing and events company.

Q And prior to that, what did you do?

A I was the director of marketing for a company called Lancope, which is now owned by Secureworks, and also a director -- I'm sorry, the director of marketing for Lancope, which is now owned by Cisco, and then the director of marketing for a company called Lancope.

Q All right, ma'am. And those businesses --

A I'm sorry, Secureworks -- I'm sorry, sir.

Q That's all right.

A Okay. I was the director of marketing for Lancope, and then director of marketing for Secureworks, which is now owned by Cisco.

Q All right. Thank you.

And what was the nature of that work?

A They're cybersecurity companies.

Q And so how many years experience do you have in the cybersecurity field?

A Since 2001.

Q All right, ma'am. Do you have any involvement with academic institutions relating to cybersecurity?

A Yes, I do. I'm an advisor on two academic advisory boards, the University of Alabama, Culverhouse Business School, their cybersecurity advisory board, and Georgia State University, their cybersecurity research board.

Q Have you ever given presentations or talks on the topic of cybersecurity?

A Yes, very regularly. I speak at many different conferences pertaining to cybersecurity.

MR. MacDOUGALD: All right. Your Honor, it may sound like I'm getting ready to qualify her as an expert, but I will not be. It's just to establish familiarity.

BY MR. MacDOUGALD:

Q Where do you reside, ma'am?

A I reside in Brookhaven, Georgia.

Q And you are a citizen of DeKalb County?

A Yes, I am.

Q You are a voter?

A Yes, I am.

Q Do you have anything to do with the DeKalb

County Republican Party?

A Yes. I'm the Chairman of the Republican Party of DeKalb County, Georgia.

Q And how long have you been in that position?

A Since April of 2021. I was reelected in March of 2023 unanimously by acclamation.

Q That organization is the plaintiff in this case?

A That is correct.

Q All right. There's a binder of exhibits in front of you, and I would ask you to turn to Tab Number 6?

A May I have my readers?

Q Okay.

A I'm not too good without my readers. And you said 6?

Q Yes, ma'am.

A Yes.

Q Tell the court what this is.

A This is our Georgia incorporation as DeKalb County Republican Party, Inc.

Q All right. Now turn to Tab Number 7 --

A (Complies.)

Q -- and tell us what that is.

A This is the DeKalb County Republican Party rules. These are our by-laws.

MR. MacDOUGALD: And for the record, let me state that these are marked as Exhibits 6 and 7.

All right. Your Honor, I tender Applicant's Exhibits 6 and 7.

THE COURT: All right. Any objection to 6 and 7?

MR. TYSON: Your Honor, we have no objection to 6. And 7, I don't have -- well, it's not signed, but I believe the testimony is that these are the rules, so I don't think we object to these either.

THE COURT: All right. I think she has identified, and it appears they're properly authenticated.

So are we marking these as A-6 and A-7? Is that what we're doing?

MR. MacDOUGALD: That would be better than the way I have them marked now; so yeah.

THE COURT: All right. So we'll say A-6 and 7 admitted -- over objection for 7.

(Exhibit A-6 was tendered and admitted into evidence.)

(Exhibit A-7 was tendered and admitted into evidence.)

BY MR. MacDOUGALD:

Q Okay. Can you describe how the DeKalb GOP is governed or how it runs itself?

A We are governed by these party rules. These are our by-laws.

Q And so when the organization makes a decision, how does it do that?

A There's a process that we do make decisions. First and foremost you have to be a voting member of our organization, and that is referred to as a county committee member. So oftentimes our executive committee will meet to bring forth proposals to our county committee for approval, and then the county committee is the decision-making authority of our organization on all expenditures, initiatives and the like.

Q All right. So the committee members are all residents of DeKalb County?

A The voting members, inclusive of the executive committee, are residents of DeKalb County, Georgia, yes.

Q Okay. Do you have non-DeKalb County resident members?

A Yes, we do.

Q And what is their status relative to the committee and the executive committee?

A They're non-voting members. They're just more of a progressive-type of membership, where they are able to attend our meetings and events, but they cannot vote on any activities or any actions.

Q Are any of the members of the party candidates for office?

A Yes, actually. We have a total of 14 candidates that are down-ballot, three that are congressional, 11 that are comprised of state senate and state house, and 11 overall of these members are voting members of the DeKalb County Republican Party.

Q All right, ma'am. As the chair of the DeKalb County Republican Party, are you aware, one way or the other, of whether your membership is concerned about election integrity?

A Yes. Our membership is very concerned about fitness, faith, integrity and trust in our elections. Many of the people in this courtroom are actually members of the DeKalb County Republican Party here in support of our petition today.

Q Does your background in the field of cybersecurity have anything to do with the positions

that you've taken as the chair of the DeKalb County GOP?

A Yes. When I was elected and reelected as the DeKalb County chair, I ran on -- my Number 1 thing was to first restore, and then ensure fitness, faith, integrity and trust in our elections, and as I mentioned earlier, I was elected unanimously both times.

Q All right, ma'am. When did you first become aware that there was an issue with encryption keys in Georgia's election system?

A I first became aware of the problems when I read a CISA, which is the cybersecurity advisory for the United States, as well as an FBI report putting out information on a Distributed Denial of Service attack on the potential for that to happen -- also known as a DDoS attack on our election communication equipment.

And I was doing research for some speaking engagements as well as some content for our programs, and what a DDoS does is a -- it is a diversion, so it is an immense amount of web traffic that brings down the front door of, basically, your website. But what's happening on the back end of your infrastructure can be very nefarious. And I was putting together a list of different types of things that would potentially happen for our program in these speaking engagements overall, so they range from ransomware, phishing attacks, as well as exfiltration and upwards type of credentialing where they take over through phishing type of campaigns, advanced persistent threats, and you have no knowledge that this might be happening on the back end, because the diversion activities of the DDoS attack take away your resources.

Q So how did the issue of encryption keys fit into what you just described?

A Well, encryption keys are basically the storage and the ability to anonymize data that is going -- and authenticate data that would be going in and out of an infrastructure or a device.

Q Is the encryption keys issue a partisan or ideological issue, to your knowledge?

A I wouldn't understand why that would be. You want to have your information stored securely. As an end user of a financial services system, like a banking system, there's an expectation that it is safe and secure regardless of your political idealogy or affiliation. When you check into the doctor's office and share medical information with your providers, again, I don't think the doctor is asking you whether you're a republican or democrat. It's an expectation that the system you're using is safe and secure in protecting your information.

Q   So when was it then that you first became aware of the encryption keys issue relative to the Georgia election system?

A   I became aware of it in late July, early August of this year.

Q   All right, ma'am. How did the party, your county party, decide to become the plaintiff or applicant in this case?

A   Well, the way -- we follow our by-laws very strictly, and my concerns as a cybersecurity professional have been raised numerous times with my members overall. So I have offered different types of best practices, quite frankly, from protecting their own identities, how we use our own passwords for applications in our own infrastructure.

So with that said, I've been educating my members for -- since I've been in office, overall. So the fact of the matter is we are equally concerned about how we are authenticating systems, how we're accessing data in the systems and everything that resides in there; so they are very concerned about it.

Q All right. So was there some kind of vote --

A Yes. Yes. So I presented my concerns to our executive committee and our general counsel outlining the encryption keys here and the passwords that are -- that are not being changed overall, and that the encryption keys themselves are static code into -- in the source code in the database, and that actually defies many best practices around cybersecurity coding overall, and in the commercial world that would actually be unacceptable.

So I presented this information to our executive committee that we pursue a legal action overall to take -- to protect all Georgians, quite frankly. My executive agreed, on the advice of our general counsel, and proceeded to present a motion to engage in litigation to our county committee members. There was a vote for that, and actually encryption keys were used. It was anonymized. In the voting we used voting technology, because we were doing this on a remote basis. And what we were able to do is overwhelmingly the majority voted to move forward with this litigation.

Q All right. Thank you.

What are the purposes of the DeKalb County

Republican Party?

A Well, our purposes of the DeKalb Republican Party is to vote DeKalb red. We are there to help our candidates. For the first time in decades, we have many candidates on the down ballot giving our citizens of DeKalb County a choice in our elections.

We want to ensure that we have safe and secure elections, and we've done a ton of work with the DeKalb Elections Office establishing a joint stakeholders organization, which is a collaborative effort with the democrats. The republicans, as well as the election office leadership have accomplished many different things. Additionally, we have built an amazing infrastructure for our members and for our candidates to be successful.

Q All right, ma'am. Does this lawsuit align with the purposes of the DeKalb County Republican Party?

A 100 percent it does.

MR. MacDOUGALD: That's all the questions I have for you, Ms. McCarthy.

THE COURT: Any cross-examination?

MR. TYSON: Yes, Your Honor. Thank you. Bryan Tyson, for the Secretary.

EXAMINATION

BY MR. TYSON:

Q Good morning, Ms. McCarthy. I represent Secretary Raffensperger, and I have just a few additional questions for you.

A Thank you.

Q You mentioned the -- that you followed the issues related to encryption in voting machines for a while; is that right?

A That is correct.

Q And you closely followed the Curling vs. Raffensperger trial earlier this year, right?

A Yes, I paid attention to that case.

Q And, in fact, you appeared on multiple media platforms giving updates on the case; is that right?

A Yes. I'm often asked to be interviewed by different media outlets to speak on a number of different topics including this one.

Q And one part of the Curling case involved Dr. Halderman's report; is that correct?

A That is correct.

Q And Dr. Halderman in his report specifically discussed issues related to encryption keys, right?

A That is correct.

Q When did you first read Dr. Halderman's report?

A After it came out in June of 2023.

Q So in June of 2023 you read what Dr. Halderman had to say about encryption keys, right?

A Yes, I did.

Q And you have, as you testified, some background and experience in those areas, right?

A That is correct.

Q And I believe Dr. Halderman's report you said was released in the summer of 2023; is that right?

A June of 2023 -- well, to the public. You had it a lot longer.

Q And you appeared on the John Fredericks show in January of 2024 to discuss the Curling trial, right?

A I regularly appear on John Fredericks' show.

Q Now you're aware that the state republican party passed a resolution about voting equipment after the 2020 election, right?

A Yes.

Q And you supported that resolution?

A Yes, I support it.

Q And you personally oppose the use of Dominion voting machines in Georgia elections?

A I oppose the use of equipment that cannot be verified and trusted.

Q And that would include the Dominion voting machines in your view, right?

A Well, actually, yes, because you cannot trust and verify our vote right now in Georgia.

Q Now, you testified, as well, before the 2020 committee chair by Senator Ligon after the 2020 election, right?

A That is correct.

Q And did you do research on the Dominion system at that time?

A No, I was a vote review panelist in DeKalb County, Georgia, and I was testifying on the lack of controls, inclusive of passwords and checks and balances, with the adjudication process of our absentee ballots.

And specifically what I did testify on was -- the fact of the matter is there were almost 900 absentee ballots that were improperly adjudicated, they had no locks and controls on them, and they were adjudicated first by a bipartisan pair, using the

Dominion equipment. Then they were put into a suspense mode to a non-partisan pair, which actually broke the laws of how adjudication is supposed to be done with absentee ballots. And that non-partisan pair -- there were no log files from them logging into the system, and we all were using the same passwords. Mind you, there were even no locks and controls on the absentee ballots themselves, allowing them to change anything -- anything on those ballots.

And the most common error of those ballots was the race for U.S. Senate, the special election that was there, where there was a jungle primary going on. So there was not a traditional nature of one or two candidates there. I believe that there were 18 candidates, and the most common error was the voters were filling in overvotes for all the democrat candidates. And it was based on a non-partisan pair who was represented by The League of the Women Voters who were actually more democrat than the democrats in the room, so they had full control of those ballots, and we still don't know to present day if those ballots were accurate.

Q You're aware that issues relating to encryption keys were raised in Arizona litigation too, right?

A I didn't follow that case.

Q Now, you mentioned you were doing research on a report on the Distributed Denial of Service attacks from the FBI and CISA when you first started doing research on this issue; is that right?

A That is correct.

Q And a D-D-O-S attack, or DDoS attack, I believe you referred to it, involves internet-connected systems, right?

A That is correct.

Q And you're aware that SEB rules govern the security of voting system components in Georgia, right?

A Yes, I'm aware of that.

Q And you're aware that one of those rules is that they cannot be connected to the internet, right?

A I'm aware of that, as well, but let me just add to that. Okay? The DDoS attack that's happening on the front door is a diversion. So what's happening on the inside of your infrastructure, whether they're directly connected or not, can be a diversion of your resources.

So the fact of the matter is, what's happening on the front door, because your website is forward facing, and if it did occur on election night, quite frankly a DDoS attack -- and several have actually -- and have already occurred in present day preeminent to it. When Twitter Spaces had Elon Musk and President Trump there, there was a major amount of web traffic activity, in addition there was a DDoS attack.

Additionally in Florida, okay, just a few weeks ago during their primary, there was an election communication company that experienced a high volume of traffic with an election that had very little election activity, making it near impossible to the county election offices that subscribe to these services to access -- for the public to access their information.

So the diversion activities that were taking place with the limited resources in security organizations across the board, exfiltration happens on the back end -- or access to systems on the back end are very obscure and often are undetected.

Q   In your work on cybersecurity you're aware that physical security is an important part of overall cybersecurity, right?

A   That is actually in tandem. So you have everything from biometrics to physical security and log files, but, you know, when I was adjudicating ballots in DeKalb County, Georgia, there wasn't even a sign-in system to the machines that I was sitting in front of when I was sitting there, or even the adjudicator that was sitting next to me. We simply signed into the elections office and were sitting there for hours and hours, and then there were batches of ballots that would come about.

So the best practices of the Secretary of State offices as it pertains to log files, password management is despicable. It would not hold up in the commercial sector.

Q   Let me ask you about the -- the allegations you have here in this case. You are not aware of any actual manipulation of election results in Georgia based on the claims you've brought in this case, right?

A   Our Secretary of State and Gabe Sterling --

Q   If you could answer "yes" or "no," and then you can explain your answer.

A   Certainly.

They remain unproven, because the fact of the matter is Gabe Sterling, our chief operating officer, I believe that's his title in present day --

it changes frequently -- as well as the Secretary of State made egregious claims on media and the public -- social media, stating that Georgia -- Georgia has the most safe and secure elections, not just in the country, but in the world. So you just put a target on Georgia's back and head to prove our elections to be safe and secure.

The onus is on the Secretary of State's office. He is the custodian of our elections, so we have the right as citizens to ensure that we trust our election outcomes as well as now verify them.

Q And my question was a little more specific. Are you aware of any actual manipulation of Georgia election results that have occurred on the Dominion system?

A There are still a lot of unexplained activities that have occurred over the last four years that are still being litigated or reviewed by our State Board of Elections as well as in the court system; so it remains unknown in present day.

Q And you personally believe that voters can never know for sure whether the voting equipment accurately reported that Joe Biden won Georgia in 2020, right?

A Well, that is correct, because you have a proprietary QR code that is doing the tabulation. That QR code, quite frankly, can't be read by a phone that reads a menu or takes you to a website, so you're asking us to trust and verify a ballot that has clear text on there, but you're not using that to be tabulated overall. I can't read proprietary QR codes and neither can my phone, which is actually illegal to have in a voting precinct.

Q And you personally would support a system where Georgia voters vote on hand-marked paper ballot, correct?

A I would support a system that we can understand and that is in clear text that our tabulation is taking place so what I enter on my ballot can be trusted, verified that is what is being tabulated on the back end, yes.

Q And you don't believe the Dominion system today provides that?

A Why would you have a proprietary code --

Q Would you answer "yes" or "no"?

A I don't trust those systems and many people don't.

Q Thank you.

And you would say as well that your goals in this case are similar to the goals of the

plaintiffs in the Curling case, right?

A No. We're simply asking for a prayer for relief here today -- trust and validation, a simple validation of the election equipment that is in place. We're not asking for it to be removed. We're simply asking for a validation by a third party to ensure that the -- that no one has tampered with anything, no one has touched anything, and what was entered in there was correct, and there's a number of ways to do that.

MR. TYSON: If I could have just a moment, Your Honor.

THE COURT: While you're conferring, Mr. Tyson, let me ask a question of Ms. McCarthy.

There was reference to -- I believe it was the Halderman report that you referred to. I haven't reviewed that. Did that ever have any specific discussion of how Georgia was handling its encryption keys?

THE WITNESS: That report was created for Georgia in the Curling vs. Raffensperger case.

THE COURT: All right. So the core of how you believe the encryption keys are being handled in this case, was that discussed in that report?

THE WITNESS: Yes, it is, and numerous other cybersecurity endeavors, yes.

THE COURT: Okay. And that was something you read when it was released in June 2023?

THE WITNESS: Yes, I did.

THE COURT: All right. Mr. Tyson, you can follow up on that or anything else and then I'll turn it back to Mr. MacDougald.

MR. TYSON: I have no further questions.

THE COURT: Mr. MacDougald, any redirect?

MR. MacDOUGALD: Yes, Your Honor.

FURTHER EXAMINATION

BY MR. MacDOUGALD:

Q Thank you.

Ms. McCarthy, to your retention in the Halderman report is there any discussion of the relationship between encryption keys on the one hand and certification standards on the other?

A There is a correlation there. The certification has to be done in alignment with the law.

Q But in the Halderman report when you read that, to your recollection does it discuss certification issues or just encryption keys issues,

if you remember?

A I don't remember specifically, but I do remember that the numerous tests were done in Halderman's lab and performed them over a several-week period, and it indicated that the machines themselves can be accessed and changed, or manipulated, both on premise and off premise; so elicit and illicit access.

Q All right, ma'am. And when did you first connect in your mind the encryption keys issue with the certification issue?

A Well, we're talking a lot about certification of elections by our board members, our state and county board members across the board, so --

Q Let me rephrase the question.

A Okay.

Q When did you first connect the encryption keys issue with EAC certification?

A Starting to dig deeper, I would say probably more in the September time frame just to get a better understanding.

Q Of what year?

A Of this year.

Q Okay. To your understanding would an exploitation of encryption keys be detectable after the fact?

A No, because the intrusion detection system that is being used, as I understand it, is the base model of the Escort, quite frankly, and would not be acceptable in the commercial private sector. It doesn't have any bells and whistles. It's simply there as a device that's adjoining to it, and it doesn't have an ability to really respond and react, and certainly doesn't have any ability to prevent any types of intrusions. You're simply relying on log files after the fact.

MR. MacDOUGALD: That's all I have, Your Honor.

THE COURT: Any recross on those points Mr. Tyson?

MR. TYSON: No, Your Honor.

THE COURT: Mr. MacDougald, may this witness be excused?

MR. MacDOUGALD: She may be excused, Your Honor.

THE WITNESS: Thank you.

THE COURT: Mr. MacDougald, you may call your next witness.

MR. MacDOUGALD: Thank you, Your Honor. We will take up the court's suggestion to put our experts up before the authentication witnesses so we can get them up and down.

THE COURT: All right. So your next witness is?

MR. MacDOUGALD: I call Clay Parikh to the stand.

(Witness sworn.)

WHEREUPON:

CLAY PARIKH,

having been first duly sworn, was examined and testified as follows:

BAILIFF: Would you please state and spell your first and last name for the court?

THE WITNESS: My name is Clay Parikh, C-L-A-Y, P-A-R-I-K-H.

EXAMINATION

BY MR. MacDOUGALD:

Q All right. Mr. Parikh, where do you live?

A I live in Huntsville, Alabama.

Q How are you employed?

A I'm employed as a cybersecurity analyst for Northrop Grumman.

Q Give us a brief rundown of your employment history.

A I've worked for all the major Department of Defense contractors. I've also done work in the private sector. I've done vulnerability management, site design. I've played "threat," which is known as red teaming or acting like the bad guy, and I've also done systems testing to include system testing in Voting System Test Labs.

Q Tell us about that Voting System Test Labs work.

A I was approached by a professional staffing company that was looking for a cybersecurity expert that had a CISSP, which is Certified Information Systems Security Professional, and I went and looked at that, and it was a way for me to keep my technical skills up, because it was to perform security testing at these Voting System Test Labs.

Q And how long did you do that work?

A I did that over a 9-year time span.

Q And -- okay. What is your educational background?

A I have a masters of science in cybersecurity. My bachelors, my undergrad, is a bachelor of science in computer science.

Q All right. Do you have any military service?

A Yes. My first profession was a United States Marine.

Q And how long were you in the Marine Corps?

A 22 years.

Q And what type of work did you do for the Marine Corps?

A I did whatever I was told to do.

Q Did any of it relate to cybersecurity or was it digging holes?

A We had security, and they're -- if you -- in the CISSP realm, there are ten domains that they talk about and they deal with physical security and encryption. I worked in what's known as the CMS vault where encryption materials were stored, so you learn about chain of custody and procedural stuff, and then of course there's always physical security.

Q All right, sir. You've covered this a little bit, but tell us anything else that you haven't told us that has to do with your professional background in cybersecurity?

A I've done the cybersecurity realm for over 20 years. I've held the CISSP for over 17 years in good standing and certified plenty of professionals under that certification. I was a Certified Ethical Hacker for, I believe, 15 years and a Cyber Forensic Hacking Investigator for 12 years.

Q All right. Do you have any experience in

performing cyber investigations in criminal investigations?

A Yes, I have.

Q Describe that to the -- what government were you working for and so forth?

A I was working for the U.S. Government, and in general terms I would just say the investigations were with -- 3-letter agencies, and one was with NASA, and the other two were Department of Defense related.

Q In the course of your training, experience and education, have you had any experience with encryption keys?

A Yes, quite extensive.

Q Can you describe the purpose of using encryption keys?

A Encryption keys are -- it's the part of -- cryptography is to keep confidentiality involved. And so you use them to encrypt and decrypt files. You can use -- they have security certificates and stuff for secured communications. It's basically a form of confidentiality under credentials management.

Q All right, sir. Are you familiar with how encryption keys are supposed to be handled?

A Yes.

Q What cybersecurity experience do you have

with respect to electronic or computerized voting systems?

A I was a security tester for several of the Voting System Test Labs during that 9-year period.

Q Did you do any test work on Dominion systems?

A Yes.

Q What is the EAC?

A The EAC is Election Assistance Commission, which was established under the HAVA -- the Help America Vote Act.

Q And this testing work -- testing lab work that you did, does that have anything to do with EAC certification of election systems?

A Yes, it does. The EAC has these certification labs. The Voting System Testing Laboratories have to go through a certification process themselves, which NIST co-chairs with the EAC --

Q What's NIST?

A It's the governing body that looks over technology and laboratory research, and they do the laboratory inspection part of the Voting System Test Labs. That's not really in the EAC's cog.

Q Is that the National Institute of

Standards?

A Technology.

Q All right. In the course of your test lab work on election systems, did you ever attempt penetration or hacking of those systems?

A Yes, I did.

Q And how -- generally, how long would it take you to get into one of those systems?

A Five to ten minutes. My best time is two and a half minutes.

Q Can you describe the difference between an insider threat and an outsider threat in cybersecurity terms?

A An insider threat -- there are basically two types. An outsider threat is someone totally out of the organization that has relatively no knowledge or access. An insider threat is an authorized person. And this can be done -- there's two categories: Accidental and intentional.

And of course intentional would be, like, sabotage and stuff like that -- negligence, that. The thing about an insider threat it not only includes the organization, it includes any contractors or vendors who have access to said systems. For example, it could even include janitors that do -- because of the physical security aspect.

Q And so the vendor of an election system would be within the --

A Insider threat realm, yes, sir.

Q All right. You have a binder on the table in front of you, and I'd ask you to turn to Tab Number 14. There's a document there that is marked as Exhibit 14 which is Applicant's Exhibit 14.

Can you identify that document?

A Yes, this is my resume.

Q All right, sir. And if you would turn to Tab Number 15. And the document marked there as Exhibit 15, tell the court what that is.

A Yes, this is the cover letter that whenever I apply for jobs that I always submit it. It includes my additional work experience and cyber experience outside of the normal DOD world of contracting, because it states, you know, I was an active member of InfraGard, which is an organization underneath the Federal Bureau of Investigation. I participated in that, and it lists the Voting System Test Lab work and experience.

Q All right. Now, you mentioned a certification you had, CISSP. Are there any other certifications that you have?

A Yes, I have the Certified Ethical Hacker and the CHFI, which is Certified [sic] Hacking Forensic Investigator.

MR. MacDOUGALD: All right. Your Honor, at this point I would tender Applicant's Exhibits 16 and 17.

THE COURT: 14 and 15?

MR. MacDOUGALD: 14 and 15. I apologize. Thank you for the correction.

THE COURT: Any objection to 14 and 15?

MR. TYSON: No objection, Your Honor.

THE COURT: All right. Admitted without objection.

(Exhibit A-14 was tendered and admitted into evidence.)

(Exhibit A-15 was tendered and admitted into evidence.)

BY MR. MacDOUGALD:

Q In the course of your work in the testing lab, did you become familiar with the requirements for an election system to be certified by the EAC?

A Yes. It was one of the very first things that I had to do. The very first laboratory I worked for was Wyle Laboratories, and they wanted to get -- to become a certified lab, and so they submitted their testing procedures to me to do an independent review, and they were going to submit that review to the EAC as evidence to help -- that their procedures were sound.

So therefore I had to read what is known as the VSS, which was under the Federal Elections Commission, it's very old guidelines, and then I read the HAVA Act itself, and did the Voluntary Voting Systems Guidelines, both I and II, that were out at the time.

Q All right, sir. What system -- election system is used in Georgia?

A It is a Dominion system, DVS 5.5 Alpha.

Q And is that system, to your knowledge, certified by the EAC?

A Yes, it's required to.

Q All right, sir. Are you familiar with the Dominion system that's used in Georgia?

A Yes, I'm very familiar.

Q How are you familiar with it?

A I've reviewed a lot of the system log information as well as four of the databases that were provided via public records request.

Q Is the EAC certification document for the Dominion system used in Georgia available on the

internet -- the certification document?

A Yes, it resides on the EAC's website.

Q All right, sir. If you would please turn to Exhibit -- Tab Number 16, and do you recognize that document?

A Yes. This is a printout of the document. Yes, 16 lists the Dominion system.

Q All right, sir. And the second paragraph of the text --

MR. MacDOUGALD: Let me -- before I ask him to read from it, Your Honor, I will tender Exhibit Number 16?

THE COURT: Objection to A-16?

MR. TYSON: No objection.

THE COURT: Admitted.

(Exhibit A-16 was tendered and admitted into evidence.)

BY MR. MacDOUGALD:

Q All right. Mr. Parikh, in the second paragraph of the text starting "voting systems," what does that tell us?

A It says, "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."

And I might add that there's also a state's requirements document that the EAC maintains. This is how the states get their HAVA grant money from year to year. That's one of the requirements of HAVA. Each state had to submit a plan, originally when HAVA was created, to the EAC and have it approved, and it lists Georgia, and in that document it states the Georgia law applicable, where it also states that it has to be federally certified and then the Secretary of State also has to certify it.

Q All right, sir. And so your testing was, as this Exhibit 16 describes, against the Voluntarily Voting System Guidelines?

A Yes.

Q All right. Turn to Tab Number 17, and there's a document there marked as Exhibit Number 17.

Can you identify that for the court?

A Yes, this is the Certificate of Conformance which is generated by the EAC from the test report that's submitted by the lab in review. They submit a certification -- certification certificate on the front of it, but they call it Certificate of Conformance, and it lists their evaluation of the voting system testing report.

Q And this is for what system?

A This is for -- it's "Model or Version: 5.5 Alpha."

Q And that's the one in use in Georgia?

A Yes.

MR. MacDOUGALD: All right. Your Honor, I tender Applicant's Exhibit 17?

MR. TYSON: No objection.

THE COURT: A-17 is admitted.

(Exhibit A-17 was tendered and admitted into evidence.)

BY MR. MacDOUGALD:

Q How would you describe your familiarity with the provisions of the Voluntarily Voting Systems Guidelines?

A I'm very familiar with them. I've actually been -- sat at the table with the EAC components that included the NIST representatives. On -- because they used to come around and audit the Voting System Test Labs and check them annually. Part of the thing is I would always get called in to speak to them, and they would ask me some questions, and I've actually commented on the Voluntarily Voting System Guidelines specifically, because, to me, they're not standards, they're sub-standards. They do not meet the level of security requirements required for systems of high importance or criticality.

Q Okay, sir. I'll now ask you to turn to Tab Number 19, and that is marked on the upper left as Exhibit Number 19, and if you can identify that for the court?

A This is the 2005 Voluntarily Voting System Guidelines.

Q And is that the version of the VVSG that was used in the EAC certification in Exhibit Number 18?

A Yes, it is.

MR. MacDOUGALD: All right. Your Honor, I tender Exhibit Number 19 -- Applicant's Exhibit Number 19?

MR. TYSON: No objection.

THE COURT: All right. Are you going to be coming back to 18, or are you also tendering that, as well?

MR. MacDOUGALD: I'm skipping 18.

THE COURT: All right. Exhibit 19 is admitted.

(Exhibit A-19 was tendered and admitted into evidence.)

BY MR. MacDOUGALD:

Q Does the VVSG address cybersecurity requirements?

A Yes.

Q Now -- and you're familiar with those requirements?

A Yes, I am.

Q What is -- do you know what FIPS 140-2 is?

A Yes, I do.

Q And how do you know that?

A I had to repeatedly read it and explain to the software developers from the vendors exactly what it meant and how they have to properly implement it, and I've dealt with multiple vendors on this.

Q All right, sir. Turn to Tab Number 20, please. And that's a document marked Exhibit Number 20 -- Applicant's Exhibit Number 20.

Can you tell the court what that is?

A It is FIPS 140-2.

MR. MacDOUGALD: All right. I tender Applicant's Exhibit Number 20.

MR. TYSON: No objection.

THE COURT: Exhibit 20 is admitted.

(Exhibit A-20 was tendered and admitted into evidence.)

BY MR. MacDOUGALD:

Q Are you familiar with how encryption keys are employed in electronic voting systems?

A Yes, I am.

Q Are you familiar with how they're used in the Dominion system used in Georgia?

A Yes, I am.

Q Are they important?

A They are highly important. That is the integrity of the whole entire system.

Q All right. And are you familiar with the EAC certification requirements with respect to encryption keys?

A Yes, I am.

Q Are you familiar with the EAC certification requirements with respect to storage and management of encryption keys?

A Yes.

Q Are you familiar with what FIPS 140-2 has to say about encryption keys?

A And their management requirements, yes.

Q Have you had occasion to examine any election databases of any Georgia counties that were used in the 2020 November election or recount?

A Yes, I've examined four databases from

Georgia.

Q What counties, sir?

A They were Appling, Bibb, Jones and Telfair.

Q Have you examined those databases from those counties with respect to encryption keys?

A Yes, I have.

Q Have you ever been qualified to testify as an expert before -- admitted to testify as an expert before?

A Yes, I have.

Q Approximately how many times?

A Related to election stuff, three times for sure.

Q And how about other cyber issues?

A A handful.

Q Has any of your expert testimony, where you were allowed to testify, related to a Dominion system?

A Yes.

MR. MacDOUGALD: Your Honor, I tender Mr. Parikh has an expert on cybersecurity, EAC certification requirements for election systems, including the Dominion system in Georgia, how they handle encryption keys and what the requirements are for certification on encryption keys.

THE COURT: All right. Any voir dire of the witness, Mr. Tyson?

MR. TYSON: Yes, Your Honor, if I could.

VOIR DIRE EXAMINATION

BY MR. TYSON:

Q Good morning, Mr. Parikh. My name is Bryan Tyson. I represent the Secretary. I appreciate your service to our country and the Marines. Thank you for that.

I wanted to ask you a couple of additional questions about your background and experience. You indicated you worked for different Voting System Test Labs that were certified by the EAC, right?

A That's correct.

Q And that you worked with Pro V&V, but you were not directly employed by Pro V&V?

A No, I went through a professional staffing company.

Q And so you were not an employee of Pro V&V, you worked for a staffing company that Pro V&V retained?

A Yes.

Q And Pro V&V is the Voting System Test Lab

that certified or -- that was involved in the certification of the Dominion system that's used in Georgia, right?

A Yes.

Q And you last did any work with Pro V&V in 2017; is that correct?

A That is correct.

Q Was 2017 also the last time you laid hands on Dominion voting equipment?

A The actual hardware equipment? Yes, sir.

Q And you've never reviewed the current Dominion 5.5A software in your role with any Voting System Test Lab, right?

A Not in the role as a Voting System Test Lab, but I have reviewed plenty of forensic reports and reports that have been evaluated and can confirm most of them are true.

Q And you've not reviewed the Dominion 5.5A software in Georgia; is that right?

A Reviewing the software -- and this is according to Pro V&V lab, they never allow security checks of the software -- no voting system laboratory, which, to me, was highly strange. Normally you test software for its functionality, its components, and the basic functions, but then it's required a security review. Because, for example, an administrative console can be manipulated, so it has to be security reviewed in how it functions, and that's normally -- I worked in a classified environment for the Missile Defense Agency, that's how it's always done, first by the software developers and then by security.

Q Let me ask a better question.

In terms of the opinions you're offering in this case, you're relying on your review of four databases, not of the Dominion Voting System at large; is that right?

A Yes, sir. But you're ignoring the fact that software development, they create an image and a versioning number, and the version used here is used across multiple states.

Q And you're not offering any opinions about the degree of risk; is that right?

A If you're asking me about the risk with these systems, the risk is high. They have no integrity.

Q Let me ask this: Did you rely on Dr. Halderman's report for any of the findings in your declaration?

A I've reviewed Dr. Halderman's report, and a lot of the vulnerabilities that he pointed out were things that I already knew and reported to test labs but never made it to final reports.

Q And you reviewed the databases that were provided to you by Voter GA; is that right?

A That's correct.

Q Are you being paid for your work?

A As far as my investigative work?

Q For your testimony and your work in this case?

A Yes. For my testimony, yes, I am.

Q And what is your hourly rate?

A My hourly rate is $250.

Q And Mr. MacDougald had asked you about courts that accepted testimony from you. Has any court ever excluded you from testifying as an expert?

A No.

MR. MacDOUGALD: That's all I have, Your Honor.

I think at this point if it's appropriate I'd go ahead and raise an objection to the scope of what's being offered here. Our motion in limine lays out our concerns of Mr. Parikh's testimony in offering opinions. Also his testimony that he has only reviewed the databases and not the software, itself -- hasn't touched the Dominion equipment since 2017. Mr. MacDougald's expansive scope of his opinions to cover everything related to Dominion 5.5, as used in Georgia, is also beyond what he should be allowed to testify to.

THE COURT: All right. Let me -- that was a lot, Mr. MacDougald, that you asked. The fields of qualification, let's just nail those down: Cybersecurity, EAC requirements, encryption keys -- did I catch it all?

MR. MacDOUGALD: Certification -- how that relates to certification, how those are used in the Dominion system.

THE COURT: All right. And other than what's already been raised in the motion in limine about the scope, how would you respond to these issues raised by Mr. Tyson concerning maybe the -- how recent his review has been?

MR. MacDOUGALD: Right. I think I might be able to address that by posing a few more questions about what his analysis of the databases entailed, if I could get a leave of court to do that.

THE COURT: I'll renew your tendering after those questions.

MR. MacDOUGALD: All right.

CONTINUED EXAMINATION

BY MR. MacDOUGALD:

Q Mr. Parikh, can you describe what analyses you applied to the four election databases that you mentioned from Appling, Bibb, Jones and Telfair Counties?

A As far as everything that I checked within the database?

Q Yeah.

A The very first thing is I restored these backup databases and was successful with all of them. Like all the other databases were, if I did not get the database, I got a backup copy, and then I compared it against other state systems which had different versioning which had the same database structure, they had a lot of the same stored procedures, which I might add are way too many, and they were the same functionality across different versions.

I can also state that I've reviewed Dominion correspondence that refers to how they handle software versioning, but I don't think that's in the scope of this hearing, but it's not -- it's not the best practice.

Q Are you -- in the course of your analysis

of these databases, were you able to run -- how did you examine them? What did you do? What tools, what software -- how did you figure out what you figured out?

A   I used everything that was on the voting system, which from a security perspective is atrocious, because I do -- all you have to do is gain access, and you're in. As my demonstrations will show, I used the tools on the system. These tools that are on these systems would not be found in the DOD operational environment, in the financial environment. There are compilers on there, there's actual where the database resides -- the management studio. These are all worst practices -- worst practices.

Q   What does a management studio mean, and how did you use it to examine the database?

A   That and the command line -- I have free access to the database. And again, they use the operating system, the Windows login credentials, which when I accessed the system, I entered without a password, which is easy.

Q   Were you able to run Dominion software as a part of your analysis of these systems?

A   Yes, and components on the software, yes.

Q And how did you do that from your machine without having a Dominion machine?

A As part of forensic investigations, the very first thing you do when you collect evidence is you create your hashes to verify the integrity of the system, you put the evidence away. You have that copy, and then you usually make another copy and you get the hashes of that, because you have to have a detailed chain of custody when you're dealing with evidence.

And usually, to expedite forensic investigations, you want the live system to pull it up. So what I did was from the image files of the Dominion system I created a virtual machine. I then easily hacked into the virtual machine. And once I logged in I had access to the database. I could manipulate the database and control it.

Q And find out how the encryption keys were stored?

A Yes, sir.

Q All right, sir. And do you think your testimony would help the court understand the issue of encryption keys and how they're used in the Dominion system and how that relates to EAC certification?

A Yes, sir, and the importance of encryption keys that they're dealing with in the X.059 [sic] certificate specifically. It's a security certificate that's used for communications.

Q And were the databases that were provided to you, are they a sufficient basis for you to form a reliable opinion?

A Yes, they are.

Q Did you apply any particular principles or methods to your analysis?

A Yes, I used standard testing methods and forensic steps.

Q And do they reliably support the opinions that you've reached here as well as in other cases?

A Yes, sir, they do. I put my declarations under threat of perjury and submit it to the U.S. Supreme Court, I stand by 100 percent of what I've written.

MR. MacDOUGALD: All right. I renew my tender, Your Honor.

THE COURT: All right. Based on the testimony I've heard so far and the voir dire of the witness, I do find this witness possesses information beyond the kind of the average layman and that on the databases he reviewed he has relevant information to share as it relates to the issues raised here, and concerns or objections that are preserved go to their weight, not their admissibility; so you may proceed, Mr. MacDougald.

MR. MacDOUGALD: Thank you. Your Honor.

BY MR. MacDOUGALD:

Q Mr. Parikh, are encryption keys any part of the Dominion system used here in Georgia?

A Yes, they are.

Q How are they used in the system here in Georgia?

A They're used to encrypt some of the user name passwords, which is not a very good standard. They should also use hashes, but they're also hashes that are weak and vulnerable -- they're left unprotected. But they use the Rijndael encryption key and Inspector as their private keys, which those are supposed to be protected. Then they also use the X.059 certificate, which is used for authentication. This establishes trust between the system components. And then there's an HMAC key that's also -- and these are all stored in the same unsecured table within the database.

Q All right, sir. And in light of how these -- when you said -- you used the word

"Rijndael"?

A Rijndael, yes.

Q Help the court understand what in the world that is.

A Rijndael was -- that encryption algorithm that's used to create those keys, there were actually three people. He was the main person that submitted for the keys, and it's an encryption algorithm. That's the industry standard.

Q And it's named after a fellow named Rijndael.

A Yes.

Q But it's spelled --

A Yes, he's Indian.

Q In light of how these encryption keys are used in the system, are they important to the security of the system?

A They are vital to the security of the system and the integrity of the system.

Q If a bad actor who has a little bit of skill knows what they're doing and has access to the system and access to the encryption keys, is that system secure?

A No, it is not.

Q Why not?

A Because they can do anything. They can decrypt the configuration files which are -- for example, the tabulator components, and so I could make the tabulator -- they could easily manipulate that and make it do whatever. They can decrypt the information coming back to the election management system -- the EMS. They can manipulate the ballot images, they can manipulate the cast vote record, they can do any number of things.

Q What is the cast vote record?

A The cast vote record contains the data, the ballot images, but it's basically the results from the tabulator.

Q Under the applicable standards of the VVSG and FIPS 140-2, how should encryption keys be stored or kept or managed on the Dominion system?

A The management and storage of encryption keys are -- when they're in plain text it's only within the cryptographic module. If they're taken out of the cryptographic module, they must be securely protected.

Q And is the way they are kept on the Dominion system in Georgia, does it comply with that requirement?

A No, it does not. They're in an insecure operating system -- information system with hundreds of vulnerabilities. The database -- and I've had database experts assist me in analysis -- that they are not configured properly, they do not log properly, as I'm sure Mr. Cotton can testify to, which leaves you hard to do a forensic investigation and determine cause analysis.

Even a system administrator tech would be lacking information. So there's lack of logging, the database -- these encryption keys would be considered confidential. It's the same thing as, like, a doctor's office who has your medical PII information or your bank that -- any business that deals with credit cards, for example, would have to protect the database. And you can protect the table, you can protect the row, you can encrypt the whole entire database, and that is not done. And to use the operating system's password and authentication to get into the database is not best practice; and again, I did it without a password at all.

Q And so how are the encryption keys, in fact, stored in these election databases?

A They're in plain text unencrypted in an insecure database.

Q And so that is not the --

A That's a violation of FIPS 140-2.

Q Because it's not in a cryptographic module?

A That is correct.

Q And does that comply with the VVSG?

A No, it does not.

Q Does that comply with the EAC certification requirements?

A No, it does not.

If I can add, the VVSG, because of the way Georgia state law states, they're not voluntarily now, they're now system requirements; they're standards. That standard is a requirement and should be mandatory, because Georgia law states that it has to be federally certified.

MR. TYSON: And I would just move to strike that last answer regarding the legal implications here.

THE COURT: I don't think we can strike anything for the record, but your objection is noted and it will be given the weight it deserves.

BY MR. MacDOUGALD:

Q Are there any particular sections of the VVSG that are most particularly applicable to the

management of the encryption keys?

A Section 7 of Volume 1 is the primary security. Security is also mentioned in Sections 4 and 6, but those -- the main importance of those deal with that. Volume 2 also talks about security and -- from an operational perspective and the risk involved.

But Section 8 talks about the quality, and they mention the life cycle management, which means it's an operational thing. Because the life cycle of any information system is from birth to death, and therefore you have to patch it, you have to do security updates, you have to meet all your requirements 100 percent of the time. It's not something where I get certified and I get connected to the network and I'm good.

For example, in my work, when they take -- I'm sorry, I've got to pause, because I've got to keep this unclassified, but -- so in the software that we develop, if they take the system off to reload the application software there's a whole process that's done, and we have configuration management. If you related it to election systems, engineering change orders.

And so when they get that approved the software developers finish their job, the techs finish their job, the last part is part of the QA where the security checks are done, and it has to be certified by the group that I worked in, the information security officers, before it can be reconnected to the network; so that's the part about quality in the life cycle management.

Q All right, sir. And so the VVSG speaks to life cycle compliance?

A Yes.

Q In what part, do you recall?

A That's in Section 8.1, if I'm not mistaken.

Q Now, would there be any point to having a standards requirement for cybersecurity that was inapplicable in the operational environment?

A No, that would make no sense whatsoever.

Q So you've had an opportunity to examine election databases from the four counties. How does it come about that you examined those databases?

A I was able to obtain them to compare them with other databases in different states that I was doing as part of the Arizona -- I don't know what it was called when it went back to the Supreme Court, but that was my evaluation. Because based on that, the investigation and the evidence found, the Arizona

Senate allowed me to get their 2020 database, as well, and discover the same inconsistencies.

Q Okay. What was your understanding of how the four Georgia county databases were obtained and made available to you?

A They were given by the counties under a public record request.

Q And how did you get ahold of them?

A In my investigation in the other system components that I've looked at as far as system log files and answering questions on what the log information did, because I was -- can interpret that and give them meaning to the components, I was made aware of them, and I asked for them to review them to see. Because, again, this is software development. This is not just specific to the state of Georgia. This pretty much -- my generated guess would be this is even outside of the versions we're talking about. It's been demonstrated --

Q Let me stop you for just a second, because I think my question may not have been clear.

How did you obtain a copy of the election databases for these four counties?

A I was given access to the Voter GA directory and then I downloaded them from there and, of course, created my hash files.

Q All right, sir. In general terms, how does the backup databases -- how do the backup databases that you obtained and then restored compare to the actual operational database used in the elections?

A It's the same database. It's the same exact database. The only difference between that and operational -- an operational database would be alive. If the system is up and functioning and that database is used on a daily basis, the backup database would be a snapshot in time.

Q All right, sir. And are the way the encryption keys were found in the backup databases, is that the same as how they are stored in operational election databases?

A Yes, it is. Yes, it is.

Q And so your analysis of the state -- the management, storage and nature of the encryption keys in the backup, is valid for operational election databases?

A Yes, it is.

THE COURT: Let me jump in on that point. So essentially what I'm hearing you say is the four databases that you analyzed and looked at very closely here, your opinion today is that is the same as the operating database that would be used live in an election?

Is that fair to say?

THE WITNESS: Yes, sir, it is.

THE COURT: And how are you able to say that?

THE WITNESS: Because these are relational databases, something that I was generated in, and they're built on a structure. And the most important thing is, is that structure cannot change because of the way Dominion implements what's called stored procedures. That's the majority of their work, and those are in the database. So you cannot change a database table, for example, and -- it would mess all the voting system up, because then your configuration of your tabulators would have to change -- there's all different components in the voting system.

If it helps to answer, in any system when they create -- and this is whether it's ES&S or Dominion, but we'll talk specifically about Dominion. They create what's called an election project, and there's certain files that get created. And one of those files in the election project is the election database, and it's based off a template, a standard, in the software development that they create from, and then it's customized. And then the table -- the table columns are given specific names that do not change, but the rows may change.

For example, if there's a state election within Georgia, it will be specific information for those candidates, their party, and the way Georgia runs their election. Even if it's for anything else -- if you're voting on funding, how to change state appropriations -- whatever, that has to go public. Anything like that, that's what changes within the database. The overall structure of the database and the procedures do not, only basically row data.

THE COURT: All right. And these four databases, they are a snapshot in time from when and what time period are you saying?

THE WITNESS: They were from after the election. A couple of them are recounts.

THE COURT: Which election?

THE WITNESS: The 2020 election.

THE COURT: The 2020 general November

election?

THE WITNESS: Yes, sir.

THE COURT: Or is it also the runoff?

THE WITNESS: There were two that are recounts, so it would have been after the general election.

THE COURT: All right. But bottom line you're testifying that with confidence the databases that you saw related to that election are still the ones in operation today? Are they still the ones being used? They weren't changed in any way in the open records disclosure process?

THE WITNESS: They're the exact same. They're a backup of that operational. For example, you have two options, sir, if you want to see that. You can bring in an election management system, which has the database on it. We can quickly do a query, it takes no time at all, and you can see structurally that is the same as what I examined, or there would be engineering change orders or a software update that say that they changed the database structure. And I can tell you for a fact that there's no such engineering change order for

Dominion systems. I've looked at every one of them.

THE COURT: All right, Mr. MacDougald.

MR. MacDOUGALD: Thank you, Your Honor.

BY MR. MacDOUGALD:

Q So let me try a short version of the questions that the court was asking.

How do you know that what -- the way the encryption keys are set up in the backup database is the same as they are in the operational database?

A Because the backup database is the operational database.

Q All right, sir.

A It's just a snapshot.

Q Now, is there some way for you to tell if the backup election databases that you examined are authentic?

A Yes, sir.

Q What is that method?

A That's by what was provided from the counties, they're verifying the hash and there's also SHA files that are in -- that are part of the system when it's created, and I can compare those SHAs to what I create and see that it was unchanged.

Q All right. For the benefit of the court,

what is a SHA file?

A A SHA file is -- it's a hashing algorithm. It's basically the fingerprint. It's the identity of the file. In file integrity you have these SHAs, hashes. There's MD5 hash, there's SHA-1, which is used by the voting system, there's SHA-512 -- or SHA-256 and SHA-512. The tool I use creates all those, because I like to cover the bases because you never know what you're going to have to deal with.

(Clarification by court reporter.)

Q What does SHA stand for?

A It's a Secure Hashing Algorithm, if I'm not mistaken.

Q That might be one instance I might have a leg up on it. So how does a hash value have any utility in authenticating a digital file?

A It's a fingerprint. It's a one way algorithm. It's bit-by-bit binary operation that covers the file itself. In systems -- and I've even read it in technical data pages -- the vendors, they recommend using a file integrity system. In the Department of Defense we have them all the time in which -- an application does it. And on your critical portions of the operating system you would create these SHA files -- these hash files, and it's the fingerprint so you have file integrity.

And part of the application thing is, it monitors the system. It's constantly checking the hashes of the system. And so, for example, if a critical application on a server is changed or modified, that will flag it, and you will get a warning in a console.

Q So I'm trying to understand the concept. Are you comparing the hashes at different times? I mean, how do you use them to figure it out?

A When the file is generated -- for example, in the public records request or when the system creates them, they create that SHA-1 file, and the SHA file is the fingerprint of that file at the time that they exported it.

Q So how -- if you do, how do you use that to determine whether what you looked at was authentic?

A You create the SHA yourself independently from what they've provided you, and you compare them.

Q And if they match, what does it tell you?

A Then it tells you that you have the file untouched and it's exactly as they gave it to you.

Q And if they don't match, what does that tell you?

A That it's been manipulated.

Q So you've said this, but I'm going to ask it a different way. Is comparison of hash values an accepted method in the cybersecurity world for verifying the authenticity of a digital record?

A Yes, it is.

Q In this case were there hash values associated with the production by these four counties?

A Yes, there were.

Q And did you carry out the process that you just described to compare hash values?

A Yes. I compared the hash on the compressed files that I got, and they matched. Then specifically on the databases in those -- because I was going to restore them -- I checked that SHA file.

Q And what did you find?

A That it matched.

Q And therefore the -- what?

A The databases are the operational databases.

Q All right, sir. Do you have copies of the -- did I ask you to make flash drives of the files that you got?

A Yes, sir, you did.

Q All right. I have those on flash drives. I actually do not have a flash drive for opposing

counsel, but I can make that available to them by the end of the day. And what I would like to do is tender those -- well, I'll show them to the witness --

MR. MacDOUGALD: If I may approach the witness, Your Honor?

BY MR. MacDOUGALD:

Q Mr. Parikh, can you identify these flash drives?

A Yes. These are the four flash drives that I put the hash file that I created to do verification along with the compressed files, and then on the same exact media I decompressed the files, per your request, so if they wanted to look at the individual pieces of those compressed files along with the SHA values; so that's what's on here. They were brand new drives from Staples purchased, so there was open package, and that was what was done. They were removed, labeled, and I've kept control of these the whole time.

Q All right. And you made those at my request?

A Yes, sir.

MR. MacDOUGALD: All right. And I would like to assign those Exhibit Numbers 25, 26, 27, and 28. But they do not have exhibit labels on them, Your Honor. They do have the county label, and so if we could ask the court reporter to put an exhibit label on them at an appropriate moment.

THE COURT: All right. Mr. Tyson, so I know we can have your conditional thoughts on the admissibility of these until you have a chance to actually look at them, but assuming they do contain what the witness says, I guess, one, I would wonder, are these some kind of sensitive materials we have to handle in a specific way, and also if you have any other general objection.

MR. TYSON: So Your Honor, I don't believe there are any sensitivities around them, as they were produced already in an open records request so they're kind of out there already. And then I think aside from us getting a copy, that's the only thing we would have -- just make sure we have that, but no objection otherwise.

THE COURT: All right. So those will be conditionally admitted. You can re-raise it if you look at the copy and it doesn't turn out to be what you thought it was, so, Mr. MacDougald, if you could provide that at some point during the lunch break.

MR. MacDOUGALD: Yes, we will get that done.

(Exhibit A-25 was tendered and admitted into evidence.)

(Exhibit A-26 was tendered and admitted into evidence.)

(Exhibit A-27 was tendered and admitted into evidence.)

(Exhibit A-28 was tendered and admitted into evidence.)

BY MR. MacDOUGALD:

Q So Mr. Parikh, what, if anything, did you do to check on the encryption keys in these databases?

A I did a general preliminary query across the database to look for anything -- I first identified the tables in the Georgia databases -- well, a couple of them were large, but still, no more than a couple of minutes to do that. Once I identified those tables, I went to those tables. I just did the basic request that's already preprogramed in the SQL database to look at the top thousand rows, and within --

Q Hold on. What's the SQL database?

A The SQL database, it is the relational database that's used by the Dominion system, and it's a relational database that uses SQL commands -- the SQL commands in order to execute, use and search functions. It's a way to organize your data and -- hopefully that's clear.

Q And S-Q-L is pronounced "sequel" in the business?

A Yes. Sorry for that.

Q That's okay.

And are SQL databases common in the world of computers?

A Yes, they are.

Q And what does S-Q-L stand for?

A It's a querying language.

Q I got another one on you. Is it Structured Query Language?

A Yeah, structured query, thank you. I couldn't remember "structured."

Q All right. I will look dumb later on, Your Honor.

Okay. So what did you -- and you did the same approach for all four of these databases?

A And other state's databases, as well.

Q And so how did you retreive -- what did you do to retrieve or examine the encryption keys?

A It's -- you can export that query from the database itself and get all the keys or you can copy and paste. It's fairly easy to get them out.

Q So there's some kind of command you enter and it shows you the encryption keys?

A Right. That query of the top 1,000 rows for a specific table, election event, it's only one row, and it identifies the election, the time of the election, the county, what type of election, and then it has those keys.

Q And what -- what is the state in which those keys are displayed? Encrypted?

A No, sir. They are unencrypted, plain text.

Q And plain text in your world means unencrypted?

A Yes, sir.

Q That means you and I could read them?

A In encryption there's plain text and then there's encrypted text.

Q Okay. And as a security -- cybersecurity professional, how would you characterize that method of storing encryptions keys?

A It's egregious. In general terms -- and I work in the cybersecurity realm, and I work with gentlemen who have got a year or two years' experience and then some who have as much as I do -- and I just say, hey, what would you think about if the secret encryption key was stored in a database in plain text? And the very first thing they say is, well, was the database encrypted? And I'm like, no. Well, how did you authenticate to the database? Well, I used the operating system. And they're just like -- their minds are blown.

Q So what does it mean for the security of the system that the encryption keys are stored in plain text in the election database?

A There is no security. For what little that you could claim is security is irrelevant. What's more important than the security is the integrity of the system. There is no integrity, because you have to understand that these keys are vital to the security and the integrity of the system. This is how you validate that it's secure, that the data cannot be tampered with. That, along with the logging, which doesn't exist -- there's not appropriate logging on these systems to even track the actions done.

Q If a bad actor got ahold of these encryption keys what could they do?

A They could change the configuration settings on the components, they could manipulate -- they can create election data and encrypt it and make it seem legitimate when the system takes it in and evaluates it. You know, there's a saying, a thousand ways to skin this cat -- there's about 2,000 ways to skin it with those keys.

Q And would such changes or such actions be detectable on these systems?

A No, they would not. And as in Dr. Halderman's -- no, they would not be detectable, and Dr. Halderman in his report refers to this, because when people ask, is there any evidence of hacking -- well, one -- two, nothing against Dr. Halderman, he was not requested to do a forensic investigation of the system. So when he makes that statement, it's not exactly accurate.

He is a security professional. I admire his capabilities, but he states when you hack these types of systems and the techniques he used would be undetectable, and I can verify that. When I did threat system stuff for the Department of Defense and we played bad guy, we would have to leave little safe files somewhere to prove, because they would swear up and down that we were not there. We'd give them a directory, go look here, and it would say "guess who was here" or "Waldo" or something silly like that.

Q Killroy was here?

A Yes.

Q All right. If you would in the binder turn to Tab 21, and there's a document there marked Exhibit 21. Can you tell the court what that is?

A It's a Security Analysis of Georgia's ImageCast X Ballot Marking Devices, and it's the redacted version of Dr. Halderman, which, for the record, its redactions were meaningless to me and some of the other technical people that I spoke with, because for a tech person it's not redacted.

Q In other words, you already knew?

A The majority of regular people, yes.

Q All right. Now, have you prepared any demonstration that would illustrate your testimony?

A Yes, sir, I have.

Q Do you have your computer up there with you?

A No, sir, it's back there. I didn't know whether I could bring it without permission.

THE COURT: While you're doing that, Mr. MacDougald, are you tendering Exhibit 21 for the record?

MR. MacDOUGALD: Actually, I think I would like to, but I don't have a witness to swear that it's -- it's an exhibit in another case. I don't have Dr. Halderman. So I'm not sure I can authenticate, but I was going to let it be a document that the expert relied on. That was my intention, but if Counsel would like to put it in, I'm certainly happy to have it in.

THE COURT: Any preference, Mr. Tyson?

MR. TYSON: And Your Honor, we would object to it coming in. It contains a lot of opinions. Dr. Halderman was subject to several days of cross-examination on it at the Curling trial.

MR. MacDOUGALD: I think that is fair. That was my thinking on it.

THE COURT: Thanks for that clarification.

Let me do a follow-up here, as well. So the statement that, you know, if a bad actor obtained the keys it would lead to severe consequences. I just want to be clear. We're not talking about the keys, necessarily, that you had as a result of the open records request. We're saying that as you believe they're currently stored -- however they're out there now. Is that what you're saying?

THE WITNESS: Yes, sir. As one of the demonstrations I will do will show you, there are common passwords. There are passwords that have been used for an extremely long time. The same passwords I saw in the Voting System Test Labs reside on the Georgia voting systems, and that's an egregious violation of password management, credential management.

BY MR. MacDOUGALD:

Q All right. And before I forget it, I have a helpful note from Mr. Olsen. Just as I was anticipating, is it X.509 or X.059?

A X.509.

Q Okay. I think earlier I think you said X.059.

A I apologize.

Q Okay. And is the X.509 considered an encryption key?

A It's considered a security certificate. It's a way of identifying and trusting a system. For example, if you go to Amazon or any of the web services, your computer -- or your phone, because your phone is nothing but a computer, is going to connect with their server, and there has to be a trust relationship built, and that's done via the certificate. And with the certificates a lot of times you really don't have to authentic with a user name and password. It depends how the system is built.

Q And have you made any findings about the X.509 certificates across the election databases that you have examined?

A Yes, I have.

Q And what have you found?

A They're the same.

Q And how would you characterize that in terms of cybersecurity?

A That's an egregious violation. And the fact that they're ten years -- they're allowed to exist for ten years, means that they could easily be reused in election systems year after year if they're not changed or updated.

Q And so as an example, on a local area network what role does an X.509 certificate play?

A It would allow the system to trust the other system that has that certificate.

Q And so the system that is thereby trusted can do what with the other system?

A It can communicate and access it, exchange communication, do whatever communications need to be done.

And another thing about the certificates, because I've had them created, it's easy to do, they are not password protected. In other words, when I installed the certificate, there's no password or pin required to install them, and that's usually a security option that you do when you create a certificate that once you import -- so that way you know it's an authorized user that installed their certificate on the system.

MR. MacDOUGALD: All right. Your Honor, at this point I would like to move into the demonstrations, but Mr. Parikh needs a minute to set up, and we've been at it for a little over two hours. May I suggest, humbly, that we take a short break?

THE COURT: All right. Yeah, let's take five, and we'll come back and pick that up.

Mr. Tyson do you have any idea, and I know we still have some ground to cover here, but how long you're going to need for cross?

MR. TYSON: I'm thinking I can do that in 45 minutes.

THE COURT: We may end up needing to break for lunch. All right. We'll be back in five.

(Short break from 11:15 a.m. to 11:32 a.m.)

BY MR. MacDOUGALD:

Q Do you have an opinion on whether the Dominion system that is currently in use in Georgia has the same vulnerabilities as these systems that you examined?

A Yes, sir, I do.

Q What is that opinion?

A That it is exactly the same. And the reason I say that is because I've reviewed every engineering change order that -- well, more than just Dominion, but every one that Dominion has ever submitted through the EAC, because the change of the database structure would require an engineering change order, because you basically have to change it across all the software versions that are distributed.

Q And if the system had been changed so as to store the encryption keys encrypted or in a cryptographic module, would that require a version number change?

A Yes, it would, because you're structurally changing that. But as I do not work in a Voting System Test Labs I can't state that. Here's what I will tell you: The Voting System Test Labs, from a technical perspective, keep things what's called de minimis, which means a minor change, so no version change is done. But the fact that not even an engineering change order has been submitted, it's, to me, evidence that the systems are still unencrypted.

Q   If there had been a change to encrypt the encryption keys or store them in a cryptographic module, is that the kind of change that would require submission of an engineering change order?

A   Yes, it would.

Q   And you have checked -- and those are filed with the EAC?

A   Yes.

And I want to state that while technically that will make it compliant with FIPS 140-2 and storage and management of the encryption keys, what it will not do is still mean that they cannot be obtained and decrypted, because the massive amounts of vulnerabilities on this system, the poor configuration of the database itself, even if you encrypted that database somebody mid-level could take over.

Q   All right, sir. And now, did I ask you to prepare a demonstration of the topics of your testimony?

A   Yes, sir, you did.

Q   And did you record that in a video?

A Yes, sir. I always record -- that's why I brought the larger laptop, because I was going to pull up the virtual machines and do it live, but considering especially network connectivity and stuff for some of the password things, you always back up and record. Ask anybody that's briefed at DEF CON or Black Hat.

MR. MacDOUGALD: All right. And, Your Honor, I propose to have Mr. Parikh play the video recording of his demonstrations and narrate them as he goes.

THE COURT: All right. Is this also something you're tendering, the demonstrative for the record?

MR. MacDOUGALD: Well, since it's a demonstrative I wasn't planning to tender it, and I do not have the videos on a flash drive, but I can certainly have that delivered to everybody.

THE COURT: Any preference, Mr. Tyson?

MR. TYSON: I don't think -- since it's just a demonstrative, I don't think it needs to come into the record. I think it's fine to play them, and he can ask questions about them. I'm fine with that.

THE COURT: All right. I know it may not need to, but there may be a preference for completeness of the record, just if you're referring to things and they're not reflected in the exhibits, or is this all it's going to be?

MR. MacDOUGALD: Well, These are illustrations of his testimony that will reflect what he's talked about, and so they're demonstratives, it's 100 percent demonstrative evidence, so that's why I didn't prepare flash drives to tender.

THE COURT: All right. Well, if there's no request by the parties then --

MR. MacDOUGALD: I'll put a flag in that and I may bring them in, because it will complete the record, and they are illustrative.

BY MR. MacDOUGALD:

Q All right. So Mr. Parikh, what is the first one we're going to look at?

A The first one deals with a common hash that's been known and is still being used, one that I saw in the lab, and so before we started I wanted to explain and brief exactly what's going on.

So I was trying to clear the screens where everyone could see. So what we have here on the left is the SQL database. Let's go back. I'm sorry. So I want to explain everything.

This is the SQL database. This is the DVS system. I've accessed -- as you can see, it's the Appling database. And we're going to go down into a table, which it's called app user. On --

Q This, what you're showing, is in the Microsoft SQL Studio?

A Yes, sir. This is the tool -- that's exactly what we're looking at. If you can see, it says Microsoft SQL Server Management Studio. This is how I access the database. And it is on the system, technically, when it shouldn't be.

On the right is a website, it's called hashes.com. This is publicly available. You can go there and use it. So what we're going to do -- I'll let it run here. We're going to go down to the app user table, we're going to select the top hundred rows, that same default query. Now, what I want to pull out, and I'm going to pause it right here, is these accounts -- and you'll see, and I'll highlight over it with a mouse -- there are certain accounts in here, if you'll notice, they all have -- they have this 0X, which is irrelevant to the key, it's just the way it stores for them, and it starts 6166 Alpha.

Notice that these are all the same.

So what I'm going to do is I'm going to show you those. I'm going to select one of them and copy, which are -- basically removes the -- out of the database. I'm going to paste it over here, remove that front portion, because that's not part of the hash.

Q All right. So let's pause for just a second. Okay? These passwords, are they encrypted or hashed or what are they?

A These are hashed passwords.

Q Which means what? Is it encrypted?

A Normally in an operating system, specifically Windows, when you put your password in and it's -- Windows does not actually store the password, unlike these Dominion database systems, they actually store the hash. So when you put in the password -- and it's a one-way algorithm, not supposed to be able to be decrypted if it's done appropriately, and even Microsoft Windows, they protect these -- and Linux, a different operating system, protects them in a different manner, they're different files, but those storage places for them are kept secure from a normal user. You don't normally see those, unless you break into the system.

And the reason that is, is because if you decrypt this hash, then you will see the password. So when you log into the system, you log in with your credentials, it automatically creates a hash and all it does is compare hashes, and there's still a hash and a whole bunch of other things I could get into on just this alone, but --

Q Now you've pasted the hash for --

A Right. On an internet site, yes.

Q Okay. Carry on then.

A And so the internet site, of course, requires a little bit of security, so they know they're not getting a bot. So we log in, and then as you can see, there's the hash, and at the end is the dvscorp08!.

Q What is that?

A That is a password that's been around for about -- I do want to show one thing in perspective of this -- but this is a deficiency report from Wyle Labs from back in 2010, and this was reported, and as you can see in there that dvscorp08 -- and again, this report that I grabbed, it's from the EAC site, another publicly-accessible site, so this password has been around. This report was from 2010. This is Dominion's. They're not the only vendor that hard-coded passwords, which from a software development thing is a critical sin. Anybody who is properly educated in computer science and software programming knows you do not do this, and so this was one of the major findings, and you can see that it's still in use.

Q All right. So going back to --

MR. TYSON: Your Honor, if I could, just since we're now referring to a different document, I feel that's out of demonstrative territory, I feel we should mark that, at least. I think he's testified as to what it was, but --

MR. MacDOUGALD: I think that's fair. I don't actually have it to mark or tender, but I can cure that -- maybe not today, because I'm not near a printer, but I will file with -- I'll submit it with a notice of filing this evening.

THE COURT: All right. Well, you potentially could also just e-mail it to our court reporter, and as long as we're looking at the same PDF, we can have it noted as -- is that going to be, what, Exhibit 26?

MR. MacDOUGALD: It would be -- I'm sorry, I'm going to go to my exhibit list. It's going to be 31.

THE COURT: 31, okay. And so if this particular document is marked as Exhibit 31, I don't know if he's identified it enough for you, but is there an objection to this being tendered Exhibit 31 later through e-mail and digital version?

MR. TYSON: Not to that method, Your Honor, but I think that we would just pose a relevance objection, but I know that's a low standard; so yeah.

THE COURT: So over that objection then.

(Exhibit A-31 was tendered and admitted into evidence.)

THE WITNESS: Sir, I can provide the full report title. It's Wyle Deficiency Report, it's T57381 Tech 01.

THE COURT: All right. So Mr. MacDougald, you are going to complete the record for us.

Now we can proceed.

MR. MacDOUGALD: Thank you, Your Honor.

BY MR. MacDOUGALD:

Q Going back to your demo, can you get back to where you were?

A Back in the DVS Corp or to the next --

Q Yes.

All right. So towards the end where the dvscorp08! was visible. And so the result of the calculation performed on this public website on the hash reveals that the password is dvscorp08!?

A Yes, sir.

Q And that's been a hardcoded password on the system since at least 2010?

A What's more importantly is, it's the password for these administrative accounts.

Q Are you aware of whether that password is in the same -- is the same on other systems?

A Yes, sir, it is.

Q In every system you've looked at?

A Every system I've looked at, yes, sir.

Q And I believe you said from a cybersecurity standpoint how would you characterize that?

A That's an egregious violation of the basic security principles. I have to state that. You can be Year 1 cybersecurity and know that you don't do that.

Q And because it's an admin password what does that mean from a security point of view?

A There are so many things that can be done as an administrator. We would take up a lot of time for me to list them. You could basically do anything you wanted to.

Q All right, sir. All right. Do you have another video? I assume we're finished with that one, right?

A Yes, sir, we are.

Q Okay.

A So the next one is going to be -- and let me pause it here to give the setup. And this is done a little bit more professional, so it's got some -- what we're doing here is, again, this is an SQL database, we're still in Appling, but we're going to run through every county, and what I'm going to show you is that even though the passwords are different and their encryption keys are different, because they're accessible, they still expose the password.

Q All right, sir.

A So on the right is another public website that does AES encryption and decryption. We're going to use the decryption portion. So the first thing we're going to do is we're going to run this query to find the keys, and this is simply it, an election event.

Q Stop there for a second.

Now we've talked in this case about you

run a SQL query and you can retrieve the unencrypted keys?

A Yes.

Q Is that what's happening in the second pane?

A Yes.

Q And so the query -- the form of the query, the computer command, is what's up at the tip top of that pane?

A Yes, sir.

Q And that's what tells the database what to show you?

A Yes, sir.

Q All right. And it's -- so just kind of walk through the query so we know what it's asking for.

A Okay. So from an initial query of where the keys are located, I identified the tables. That's why you see it says "from election event." That's the table that's shown. And then in the other demo where I was going to do live, I would show you that table at first, but it's got a lot of extra things, and you only want to see the keys.

So this is that query. It pulls up all the pertinent keys. The one thing I want to stress, and for everybody to pay attention that watches this, is pay attention to the X.059 certificate data.

Q Okay. Before you go on, it says "select name" and then it's got Rijndael key, Rijndael vector, X.509 data, HMAC key?

A Yes, those are the column names for those.

Q And so the effect of this query is to tell the system to go to the election event table and show you the Rijndael key, the Rijndael vector, the X.509 data and the HMAC key?

A Yes.

Q Thank you. All right. Carry on.

A So we've got the key, and you can see you're partially blurred out. Now, as we cut and paste those in, we're going to go over -- now we're going to go for Appling, and we're going to query, and I'm going to pause it right here. We're querying the tabulator user.

So these are the passwords for all the different tabulators. And the thing that needs to be noted is they're all the same log in, and notice they're all the same password. And again, they're encrypting passwords, which is ridiculous in itself. But -- so we're going to -- now that we have that, we're going to put that in the encrypted text --

Q All right. Pause there. Pause there.

So to summarize where we are, you retrieved the Rijndael key and vector --

A And vector, yes, sir.

Q -- on the system from the election events table. You pasted those two values into this -- the appropriate fields on the web page?

A Yes, sir.

Q And now you've gone and selected a password, an encrypted password, from the user table?

A Yes, sir.

Q All right. And then what do you do with the password on this web page?

A This password?

Q Yeah.

A Is used for the administrator to log in to the -- oh, you wanted to see it execute?

Q Just explain what's happening on this web page.

A All right. So if you see down at the bottom -- and again, I partially blurred it out -- this is one of the passwords in plain text. So this is what the administrator, when he goes to log in, the pin that he would put in to run that tabulator.

Q And so what this demonstrates is that you

can retrieve the encryption keys, which are in plain text, and use them to decrypt an administrator's password?

A Yes, sir.

Q All right. Carry on.

A So what we're going to do is now we're going to go back, we're going to pick Bibb County, do the same thing. We execute the query, we get that, and notice --

Q Hold on one second, Mr. Parikh.

When you execute the query, the result is displayed below the query in that middle column?

A Yes.

Q All right. And so it's a row with columns, a single row with columns?

A Yes, sir.

Q And the columns are?

A The columns are -- the application calls from the column and per the row -- it makes -- the software applications make queries to these databases, so it's got to identify what data to pull, and so the application will say, hey, I go to Rijndael key, because I need an encryption key for a certain administrator, and then basically it would write this stuff there. And it's got to verify -- the encryption key has been used for verification, to decrypt the files once they're taken on, and so --

Q All right, sir. And this result that we see, those are the encryption keys in plain text; is that right?

A Yes.

Q Okay.

A Decrypted at the very bottom -- of course I've blurred a little bit of it out.

Q But over in the middle column the query result is showing you encryption keys, right?

A Yes.

Q And they're in plain text?

A Yes.

Q Okay. And that's how you're able to use them to decrypt the password?

A Yes.

Q All right. Carry on.

A And so we'll go back over, we'll execute the same query to find the tabulator users. And as we can see, a lot more tabulators here, but again, all the same password. So while we're cutting and filling and pasting in, I want to pause it right here, because this is important from an auditability standpoint. You've got the same password and the same account logging in with no traceability as to who did what. It only takes one nefarious person, one insider, to do something, and then it's game over. He can do it on -- he or she can do it on every component. This is very poor credential management.

Q Does that comply with the VVSG?

A No, it does not. The VVSG states to use best practices, and this is not a best practice. It's a worst practice. And we'll run through each and every county, again, pay attention the X.059 certificates being the same across different counties. And you see they're different keys -- we get a different password in each county, but they're still all easily done.

Q All right, sir. And that's the end of that one?

A Yes, sir.

Q All right. And have you got another one?

A Yes, I've got one more.

Q All right.

A All right. So what we've got here is I'm going to do a little bit of what we call key math as I'm going to refer to it. This is the database, Appling again, pulled up. I want to point out that -- and I've already executed this other one, several people have, of just flipping the vote. And the reason I kept talking about the X.059 certificate is because I'm doing these things manually. This data can be collected -- I can do these queries remotely.

There's also a command line back in for studio management, which is on the system. So this stuff, once you've got connection on an internal network to the system, then this is easily done. This could be put on a USB drive.

For example, USB drives are small. Our wireless devices for our Northrop Grumman corporate laptops -- because where I work, we can't have them internal. They remove them, because that's the only way to shut it off. Then you get a little -- it's the same size as my mouse, plug in for the USB. That's the wireless card. So that's how small. On that wireless card I could also put -- I could put the wireless card, I could put an application to make it think it's a keyboard, redo the commands -- all this in the background. I could put in a phone cable card, in the power card, in the printer cord -- that's how easy it is to put the scripts and execute them on the systems.

And I want to bring that out, because that's where manipulating one digit for two candidates in that table, which would be least notable than this. So what we're going to do, we're going to go down here, we're going to go to the stored procedures, which is where the majority of the work -- what I want you to see is, I did not open the other folder. This is just the stored procedures that are ran in the database for the application to work -- a ton of them, but we're going to go to contest results. We're going to execute the procedure.

Now, what I'm going to do here, I'm putting in a variable, because the application would do this in order to make it execute, it would send this automatically, and so what we're doing is we're putting in the variable so we can run it. And as you see here, you see that Donald J. Trump got 6,526, Joe Biden got 1,779.

Now, I'm going to use SnipIT, because I don't have that great of memory. We're going to cover this up so we've got it frozen. We're going to downsize that. Now I'm going to go back and I'm going to modify the actual stored procedure with just a few lines of code. So we're going to scroll down toward the bottom, all the way to the bottom, right before it goes -- and I'll show you when we get to it. I'm going to pause right there. Notice, Print 4 is "add totals finish," so we're going to submit this right before all the totals are calculated. And so what we're going to do, I'm going to put a hard return in there -- that's hitting "enter," and then I'm going to -- I've already got the instructions to make this quicker and expedite it, and so I'm copying these instructions and pasting them in there.

And we're going to pause this right here. Notice that Choice ID Number 2 is getting a thousand votes taken away and Choice ID Number 1 is going to get a thousand. So I'm going to execute it, so now it's functionally stored, and then I'm going to go over here -- we see how the totals are -- and now we're going to execute this again, and we see that the totals have changed.

Q And how -- okay.

A And right here we're comparing them, so -- from the screenshot -- so you can see that it changed. This can be done on any race -- anything, and this is one of the 2,000 ways to skin this cat.

Q All right, sir. Would the encryption keys allow a bad actor to perform this exploit without detection?

A Yes, sir.

Q And that's the third and last demo?

A Yes, sir, it is. Unless you wanted to see the decryption of the DVD files, but that's a little bit more complicated -- it's not complicated, it's easy to do, but we would be seeing it in the command line terminal, not the application itself, so I think for most people who aren't nerdy, they wouldn't -- you can see the candidates names, choices, and stuff like that, but --

Q I think that one is a little too nerdy for us.

A Yeah.

Q We went to law school for a reason, which most of us it's because we're not good at math.

Okay. Now you've already talked a little bit about the dvscorp08! and the common passwords. Talk about that in terms of the VVSG and certification requirements and what kind of risk it creates.

A It's a significant amount of risk. Now the VVSG states that you're supposed to use best practices for your authentication methods, and this is definitely not one of them.

The worst thing is in my investigations of the database I've seen that these user names and passwords are the same in other states. So what that means, for example, someone from Arizona or Colorado could just wander in or they could share that account information that has it. So what we've -- so by them being the same -- not only just in the state of Georgia, but with other systems, it allows -- now the password can be known by anybody.

So you get somebody in Colorado who says, hey, calls their friend in Georgia, and boom, it's over, because they can access. They have the credentials. They don't even need to go through this. They're already going to be able to get on the component and then do whatever they need to do.

Q So the password in Colorado is the same as Georgia?

A Yes, sir. In my declaration to the Supreme Court I actually highlight and show those.

Q In light of your testimony about how the system in Georgia does not comply with the requirements for certification, can you help the court understand how it got certified?

A I can simply state what I've stated for a while that the certification is simply more than a rubber stamping outfit. There's a reason I left in 2017, because I did this to keep technically proficient. I got to create different versions of virtual machines, I hacked in -- matter of fact, it's sort of like a rock star to the labs, because when I showed the guys the simplest things they'd never seen done before. I can tell you I taught them about how to test tamper seals, because when I started there weren't security seals on the voting systems. I showed them how to pick locks, because most of the locks on these tabulators are what's called wafer locks, which are easy to pick. I've shown -- we've -- actually using an alligator clip from things, showed them how to encrypt a secured storage compartment for poll books. Those are the things that I taught them.

They have no security people -- and again, I went through a professional staffing company, you know, not a full-time employee. I was the only security person. I cannot speak for SLI, but for Wyle Labs, which translates to NTS, which no longer -- well, NTS still does the hardware portion for them -- for Pro V&V, and Pro V&V, they have no security professionals in there. They barely comprehend software quality testing, let alone security testing.

Q As you understand the VVSG requirements, is it a continuing obligation that election systems used by the states meet those standards?

A Yes, and you should be able to meet those very low standards.

Q Is there any reason that -- well, why don't you tell us whether these Dominion systems can be brought into compliance with the certification requirements for encryption keys?

A They could be. I'm highly doubtful that it would be any time soon. My suggestion is to have a mitigation plan in place and to make the appropriate engineering change orders and modify the logging and stuff and make it more transparent and more viewable.

Allow these logs -- and again -- and I state this as a systems person in IT with over 20 years -- system logs are not proprietary. They contain no confidential information within them. DOD even makes sure they have a standard that you can't even have the user name or the password in the same log file. What you do find, and I'm just going to give you this example, when you put your password in as your user name, we still see that in the log file, so then we have to look at another -- and we remind that user, please go change your password, because you've just identified -- and we're the only ones in security that see that. That's the extent as far as critical infrastructure in the DOD realm goes.

Now, voting systems have been deemed critical infrastructure by the Department of Homeland

Security, but yet we don't make them maintain and follow the same critical infrastructure requirements. That's what I'm saying, if the Dominion voting systems can't meet these low standards, it's bad.

So mitigation, you open up the logs, you allow transparency, you start doing the logging and you put those steps in place to allow trust and confidence to come back into the elections to make it more auditable.

Q Are there any other transparency or disclosure measures that would help mitigate the risks that you've identified?

A Yes. I've started a fairly detailed list, but that's pretty lengthy, and that would be something that -- I'm unsure -- I believe the state election board -- I know they do rules. In Alabama, our state election board approves the engineering change orders, and so, to me, it would be the state requesting engineering change orders to make these small changes as far as logging auditability, and then on the county or the state's behalf to make sure that they're public records so that they can be checked by a third party.

Q Would it mitigate any of the risks you've identified?

A It would help you identify that the risk occurred and actually pursue and possibly identify the perpetrators or the cause of the incident.

Q So let me ask you this: If there was a requirement to produce promptly system logs, ballot images, and cast vote records, would that help?

A Yes, sir, it would.

Q And would that change the voters' user experience on the machines in any way?

A Not in any way, sir.

Q And do those records already exist in the ordinary operation of the system?

A Yes, sir. The only thing that I would add on that is to ensure that all ballot images are retained. A lot of them -- to include my own state -- do not retain them all, and to me that is a digital chain of custody infraction. You've lost the chain of custody. You're taking something that started as a sheet of paper that went into a tabulator, it's transformed -- a picture is taken. That picture is what's analyzed by the software. It's now in digital form.

Every process of the digital form, which would include once that image is taken, all the hash files there. All the identifying fingerprint signatures for each file to show that it is not manipulated, because it can be manipulated, and you track it all the way through. And all that stuff should be auditable -- but to have those images, it should be required.

I complained about this when they started allowing vendors the options in the states to turn the option off. Because too, you're evaluating the ballot differently from one voter than another.

Q   Do you have any understanding of whether HAVA imposes any auditability requirements?

A   Yes, sir, they do.

Q   Of the nature you've just described?

A   Yes, sir. They require all system logs, and those are often not provided. The best way to actually get them sometimes is to grab an image of the file so then you get the operating system logs and all that. Any forensic investigator will tell you this. You need all the possible data you can get, and this would include any components.

Q   And producing the records that are already maintained by the system in the ordinary course, to your understanding does that impose any significant burden on election officials?

A   No, it does not.

MR. MacDOUGALD: That's all the questions I have for you, Mr. Parikh. Thank you very much.

THE COURT: All right, Mr. Tyson. Why don't we get started and see how much headway we can make.

MR. TYSON: Certainly.

EXAMINATION

BY MR. TYSON:

Q Hello again, Mr. Parikh. Good to see you. All right. So I wanted to kind of drill down a little bit. As I understood your testimony, you're offering opinions about the storage of these encryption keys and the compliance with both VVSG and HAVA.

Is that fair to say?

A Yes, but the main thing is about FIPS 140-2, which the VVSG require.

Q And so it's your conclusion essentially that the EAC improperly certified the Dominion equipment that's in use in Georgia, right?

A They took what the Voting System Test Labs gave them. What I will tell you is that system testing is incomplete and not to par. And I -- whether it's considered -- I've got it from Wyle employees, to include the same employee who started

Pro V&V, told me --

Q Let me stop you before you give hearsay testimony here. You can't tell me what somebody else said.

A All right.

Q So I can just be clear on this, you're not saying that the Dominion 5.5A system we use in Georgia is not EAC certified today, right? You're just saying it shouldn't be, right?

A It got an EAC certification.

Q And that certification has not been revoked, correct?

A That's correct.

Also not followed is the EAC's election guidance in that the components should be suspended until an investigation is done before it's utilized in an election.

Q So from your perspective the EAC made a number of errors when it certified and did not revoke the Dominion 5.5A system, right?

A So I have to explain this, and again, I'm not an attorney or a lawyer, but I did read the Help America Vote Act, and when I first saw Voluntary Voter Systems Guidelines I said, well, why are standards and requirements voluntary? I'm from the DOD world, and so bear with me on this, so I'm used to requirements, you follow them. If they're standards, you follow them. You get certified, you meet them all. If they're voluntary, I had to go back and reread the constitution, because the federal government cannot dictate to the states how they run their elections, and that's why they're voluntary. But once the state says that it's their requirement to be federally certified, then it is a requirement. And so, necessarily, the way you're leading it, also -- you would have to include the Secretary of State failed before I would say -- but both those parties.

Q But an EAC failure is part of what you're talking about, right?

A As well as -- yes, sir, as well as the Secretary of State.

Q So let's talk a little bit about the EAC certification process, because I believe as you testified the EAC certifies different voting systems, right?

A Yes.

Q And the VVSG 1.0 standards are the standards that all current voting systems are certified to, right?

A Are you specifically talking about

Georgia?

Q I'm saying as a general matter, do you know?

A No, there are actually other certification levels. Less than a handful.

Q But VVSG 2.0 has only been adopted recently by the EAC; is that right?

A That's correct.

Q And in order to get certification by the EAC, the EAC also certifies Voting System Test Labs, right?

A That is correct.

Q And Pro V&V is a certified Voting System Test Lab by the EAC, right?

A Yes, they are.

Q And when the Voting System Test Lab makes its report to the EAC, and the EAC certifies, there is then a version of the software that is retained by both the Voting System Test Lab and the EAC to say this is kind of the gold standard software, right?

A The Voting System Test Lab actually retains that.

Q Any change in the voting system that's more than a de minimis change that you referenced requires a new certification, correct?

A That's not necessarily true. There are varying parts of the changes, but most of them do, yes.

Q And that would include even, for example, installing an operating system software update that could require a new certification from the EAC, right?

A Not necessarily true.

Q But it could, right?

A It could.

Q And as I understood your testimony there were two main areas that I understood you to say didn't comply in your view with the VVSG standards. One was the storage of encryption keys, and the other was the reuse of passwords.

Do I have that right?

A That is correct.

Q And you'd agree that on the Dominion system encryption keys change with each election, correct?

A As I demonstrated in the video they were different between each of the counties within Georgia, but that's irrelevant to the point because they're unprotected.

Q So just so we're clear for the court, it's your understanding that in each election each county

has a unique encryption key, and then each of those encryption keys also changes, not just between counties but also from election to election, right?

A Speaking specifically about Georgia, but in some Dominion systems that's not the case.

Q But in Georgia it is, right?

A Yes.

Q And so if someone had the 2020 encryption keys for Bibb County, Georgia, they would not then be able to access automatically the 2024 Cobb County election database; is that right?

A Well, if you're talking the keys, there's a reason I've talked about the X.059 certificate being the same and good for ten years. You don't have to have the keys, necessarily, to get to the system. Once I get to the system, I get the keys.

For example, let's go off what you said, the 2020 keys are irrelevant. But to get them you know where you got them from and how you acquired them, it would only take you a minute to get the new keys.

Q So let's talk about that key, because you have to have physical access to the election management server to get that database?

A Not necessarily, no, sir.

Q Okay. What non-physical access method could you utilize to obtain the election databases?

A Would you like me to go over the five APTs for standalone air gap systems within the last ten years or the recent one where they exfiltrate data from the sound from the color from your monitor? That's a way.

Q So it is your testimony that anyone without physical access to an election management server can access the database?

A I did not say anyone, sir. So what I'm telling you is, if you rely on physical security -- and by the way, I'm a physical security subject matter expert in the state of Alabama, I do know a thing about it, you are already gone. You cannot rely on physical security.

As someone who has looked at some of the voting locations that are run by counties, they're improper. They do not meet regular physical security standards, so they're not really secure facilities. These systems aren't stored. There are improper procedures on how the voting systems are stored and the auditability of when they start them up.

So not anyone, but the majority of people who watch a few YouTube videos on vulnerabilities and spend a couple of hours on research -- and again, we're talking about critical infrastructure for a trillion dollar economy, it's fairly easy to do.

Q We can agree that new election project files are created in Georgia for each new election, right?

A Yes. You have to create a new project file. It's specific to the election.

Q And part of an election project file is a new election database like the ones you reviewed, right?

A No, sir. It's a new database, that's correct. The structure of the database and the composition of the database remain the same. You have a template to where the data that you put in for the election through the EED, in Dominion's case, the Election Event Designer, you put all your data into that, it does the configuration for that specific database, but the structure, the keys are stored in the same manner.

Q Just so we're clear, the structure of the database is the same because that's the Dominion system's method of using that database, but the information in that database would be different for each election.

Is that fair?

A Yes, sir. And it's still unencrypted and in their quote/unquote database.

Q And that would involve different candidate names and different races that are in the database, right?

A That's correct.

Q And it would involve different encryption keys, as well, right?

A Not necessarily. If you had a lazy county worker that wanted to use the same encryption key, just like we see they use the same passwords, that could be done.

Q Is it your understanding that county officials in Georgia build election project files?

A No, sir. But that leads us down another path with the way the technical data packages, which I've reviewed plenty of, and the way these things are sold, I will tell you -- and this may be irrelevant to Georgia, but my state of Alabama, we violate our state constitution by having it contracted out with a third-party vendor.

So what I will tell you is, many counties let the vendors access it, and again, a vendor, a contractor, is an insider threat.

Q So you don't know how election project files are built for Georgia elections, right?

A From what I've gathered, I'm not 100 percent on, but they are created by the vendor.

Q And you've never reviewed the process that Georgia uses to deliver election project files to county officials, right?

A That process specifically, no.

Q And you've never reviewed the process that counties use to test voting equipment with logic and accuracy testing for Georgia elections; is that correct?

A Logic and accuracy testing are nothing but a semi-weak functional test of the system. They have absolutely no security relevance. What you would do prior to an L&A test, each election, you would do an acceptance test or a trusted build test, which only does file integrity and basically says I've got the software I'm supposed to have, and that's on the base system.

But because you have an election project, that's going to change a few things, so the limited hashes that they provide the counties to validate that, it probably would be irrelevant. But to say that logic and accuracy -- I refer to them as a dog and pony show. It's a warm and fuzzy.

Q But to be clear, you have not reviewed -- even though you don't think they're valuable, you haven't reviewed Georgia's logic and accuracy processes, right?

A No.

Q And you haven't reviewed the process that is used -- well, let me go back.

In terms of the election project file, what you are looking at in the demonstrations you showed us was a post-election file, correct?

A And you keep referring to it as the project file. You mean the database?

Q Right, the database.

A Election database, yes.

Q And in order to manipulate what's in the database, you would need to get access to the system somehow and then you would need to then get to the encryption keys; is that correct?

A That's correct. Easily done.

Q And then the individual who -- or hypothetical person we're talking about -- would need to obtain access to each component of the system if the program file had already been distributed out to those components, right?

A Not necessarily. Again, there are literally hundreds upon hundreds of attack vectors. Based on the data in the different counties I've examined in Georgia, I would say there's at least six different attacks that occurred -- or techniques in the attacks. They did different kinds and different methods. And again, that's because you know your target.

Some counties are larger, you evaluate the processes and procedures, and you find where the vulnerabilities are. So my review of processes and procedures, which I bet would be lacking, like most other states where I have reviewed it, would be that, but it's irrelevant because the keys are in a highly-vulnerable system with hundreds of vulnerabilities in an insecure database unprotected.

Q And you mentioned several times the different attack vectors. You don't have any evidence that anyone has ever manipulated any of those attack vectors in a Georgia election, right?

A I will reiterate what I said earlier that Dr. Halderman has reiterated. If you do some of these vulnerabilities there will be no detection, especially in a system that does not upsize the logging information and constantly overrides the Windows logs.

These are not best practices. You cannot audit or track down anything. Half the logs are not recorded. The application logs that are developed are improperly done anyway. They don't even go down to the millisecond, which is a best practice standard.

Q So to be clear, my question was a little more specific. You don't have any evidence that anyone has ever utilized these attack vectors in --

A There would have been --

Q Excuse me. In an actual Georgia election, right?

A There would be no evidence.

Q So you don't have any, right?

A Of course you're not going to have any. But if I attacked them, you still wouldn't have any.

Q And it's your testimony that even if the encryption keys were stored in an encrypted way you would still consider the Dominion system to be vulnerable to attack, right?

A It would decrease the likelihood, because you're going to knock out the low-level key scripters; that's why.

Q But I believe your testimony was that there would be a long list of things you would want to see changed in the Dominion system to make it more

secure, right?

A It's a detailed list, and as I do when I provide -- and I've provided it for counties in Arizona and other places, because, believe me, I think my folder count for different states is 26 currently, and people ask for help, and so I do that.

A lot of it is process/procedure reviews. That's why I'll state L&A testing overall are a farce. And so -- it's dependent. I started writing one specifically for Georgia, because I told them I don't think the vendors will come through in time, so you've got to do -- we do it in the Department of Defense, they do it in Health & Human Services, Department of Labor and all the other programs and agencies I've supported. You have to have a mitigation plan.

If you can't fix a vulnerability and remediate it on the spot, you've got to have a mitigation plan. Every agency in the Department of Defense has to report backup those plans, and in a timely manner, and it depends on the criticality.

What I will tell you is, is based off what I saw the EAC and the states talk about between some Governors' e-mail and the remediation times -- oh, I think it came from CISA -- those remediation times were obnoxious, and then they try to keep it secret from the public on the mitigation of these vulnerabilities; so it's just ridiculous.

Q So I believe your testimony was that there was a production of ballot images, logs and cast vote records, that that would help this mitigation --

A Yes, it will.

Q -- you're talking about?

But you would agree that wouldn't address any of the undetectable hacking you've testified about, right?

A It would help identify that something happened. There are different things that you can do. For example, you can just look at the election data as precincts come in and analyze from a mathematical standpoint. You cannot fight math. It can only do certain things. So -- and I'm talking from a security incident response, a security operations center perspective.

If I saw some of the anomalies like I've done in the different states in the elections, you see that, you immediately notify the server team, image that server, capture that network traffic. We have to analyze because there's an anomaly there, and you have to investigate. There's been no investigations of any detail. And even if you do, the way the systems are built and configured they do not log it, and so it's one thing to try to find the evidence -- and you keep going on the evidence, and I and Dr. Halderman have said there will be no evidence.

But the thing is about the trust of the system. Would you put your money in something that you couldn't guarantee wasn't hacked? It's crazy to base it on that and trust a system that has no integrity.

Q Is it your testimony that Georgia voters cannot trust the outcome of the 2024 election if this system is used as it's currently configured?

A Yes.

Q And in terms of the various pieces, you said, of things you analyze and look at, you'd agree that's kind of a policy decision of where you're going to put resources to investigate; is that right?

A I'm not quite sure I understand your question.

Q Sure.

So we were talking earlier about the cast vote records, the ballot images and the log files that you believe should be made available. You'd agree that how many resources to devote to those types of investigations is a policy question, right?

A It could be considered a policy question, but again, these voting systems are paid for by tax money, which is the voters, and so to make something publicly available -- and if you look at HAVA, Title III, Section 301 and the requirements of Section A, a voter not only has to verify and independently check his ballot cast, that voter has the same right to ensure that his ballot was done that. And it varies from state -- I've read a lot of state constitutions, and so that varies, but that's something that should be done anyway.

Now if you're trying to go off the way Fulton County said about it would take them 50,000 hours to gather data, I could pull two dozen database people that could show them how to do it in an hour, and so resources to access public records and to extract these logs and back them up and put them somewhere secure for people to be able to request them is not that labor intensive.

Q Let's talk a little bit about the data and the pieces here. When did you download these Georgia databases that you began your review on?

A I don't know the exact date. It was a while back prior to our submission for the Lake/Finchem case to the Supreme Court.

Q And that's the Arizona case that you were referring to?

A Yes.

Q So at least several months ago?

A Yes.

Q Do you recall when you started preparing your declaration for this case?

A It was somewhere in between my trips to the -- I've come here several times to talk to the state election board on behalf of some of the complaints there, I've been asked to speak and I've been asked technical questions. And I do -- I will give Georgia kudos. At least your state election board is listening to the voters and hearing things, unlike my home state.

Q So it would be safe to say probably several months is when you started on the declaration, as well?

A I would -- probably after late July, I think.

Q Do you recall when you first identified the encryption keys being stored in an unencrypted way in Georgia?

A In Georgia was when I got those -- when I got those databases. I saw the same exact thing that

I saw in Arizona and Colorado.

Q And had you reviewed Dr. Halderman's report from the Curling case before you downloaded those databases?

A When was that released?

Q I believe it was the summer of '23 was the testimony?

A Yes. People -- I got several copies of it. People asked me to review it and give my opinion.

Q And you're aware Dr. Halderman discusses this encryption key issue in his report, right?

A Yes, he does.

Q So is that when you first learned about the encryption key issue, not when you looked at the databases?

A I knew -- I knew there were issues with keys from other reports, but then again, knowing this vulnerability and the amount of stuff that was going on in different states, it didn't register until I really focused in on the Kari Lake case, and examining that, and when Arizona wanted their database examined.

Q And the Kari Lake case that you referenced, the court didn't order any relief in that case, right?

A No, they did not.

MS. YOUNG: Your Honor, it's about 12:30. I'm about to shift to a different area. It might be a good break point.

THE COURT: It is a good stopping point. Yes, let's take a lunch recess. It will be somewhat abbreviated; hopefully folks packed. Let's take 45 minutes. So let's be back, ready to go, at 1:15. I'll instruct the witness that while you can discuss the matter with counsel, not to discuss it with any witnesses in this case that may testify here.

For the parties here, if anyone wants to assemble in the jury room over the lunch break they also can do so. We also have a side room that may hold about four. I'll let y'all arm wrestle over it.

We'll be back at 1:15.

(Short break from 12:30 p.m. to 1:15 p.m.)

THE COURT: All right. Let's go back on the record. Sir, I remind you you're under oath.

BY MR. TYSON:

Q I know you worked in the security world for a long time, and Mr. MacDougald had asked you some questions about is the system secure or not.

You'd agree that security is a matter of degree. Something is not secure or insecure, it's, kind of, more secure or less secure, right?

A Correct.

Q And part of understanding the security of any particular system involves looking at some of the cybersecurity components, right?

A Yes.

Q And it involves looking at the physical security of those components, right?

A True.

Q And in determining how a system functions, you'd agree that sometimes usability for users can be kind of at war with security at some level, right?

A In certain aspects. But in system design, if you create the system appropriately, usability is already taken into account, so security never really hampers anything.

Q And part of the EAC's review of voting system includes its usability both for voters and for poll workers, right?

A But we're talking about critical infrastructure, the thing that decides who you put in office, who you vote to protect you as Sheriff, how you fund your parks -- that's critical. Those are high-value systems. You don't put security in the back end of it and say that usability is going to be paramount over security.

Q Well, my question wasn't which was paramount, just that part of the EAC's review of a voting system includes usability, right?

A Any system that gets evaluated, it's usability and security and all that -- not just in the technical world, in any process or procedure.

Q And there are sometimes where you may make a choice that makes a system more secure but less usable, right?

A Yes, but what we're talking about as far as these systems doesn't make it less usable. I would care to sit down with any of the vendors and talk that technical conversation.

Q And so when we're talking about voting systems, just to come back to the main point, we're not talking about whether a system is -- the Dominion system, for example -- is secure or insecure. We're talking about if it's more secure or less secure, right?

A No, it's not secure at all.

Q So in your view, it's not an issue of degrees of security as to the Dominion system, it is

just straight up insecure?

A Yes. As I've stated before, your home computer is more secure, but I don't know about your work one. As you're an attorney, I often find that attorneys don't even use hard disk encryption on their laptops, which is another issue I have, but that's a side note. Please do it if you don't. Your clients will appreciate it.

Q But again, when we're looking at this, what methodology did you use to reach the conclusion that the Dominion system is insecure -- not just less secure than you would like it?

A The primary factor are the keys stored the way they are. They're within the operating system and the outdated applications. When I say there are hundreds of vulnerabilities, there are hundreds of vulnerabilities. And I've done this analysis on different machines -- for example, ES&S in my home state of Alabama, just between the operating system and the database server, 330-something vulnerabilities, and that's a conservative estimate. There's other things about your transport protocols, the SSL version being used, all those other things -- there are literally hundreds of vulnerabilities.

Q And you'd agree there are many

vulnerabilities from any election system a jurisdiction chooses, right?

A Yes.

Q So let's talk a little bit about the data that you looked at. I just want to make sure I understand the pieces that you downloaded from the website from Voter GA.

You mentioned those were SQL files. Was it just the databases or was it the entire election project that you downloaded?

A They had other elements in it. They had ballot images in it, .tif files, and there are other components. There was a package, info.xml, which allows -- because with the SHA file of that I was able to check time stamps of the other files to know that they hadn't been tampered with. Because if the XML has not been tampered with, it had the time stamps of the files for some of the stuff. There are multiple things.

Q But the pieces that you were analyzing were only the databases, not those other components; is that right?

A I looked at them. I have analyzed the .tif files, because I've done calculations on how much it takes to transfer the image files and how some counties in Georgia don't do it until the next day, which is an improper procedure. It's different even from what is called for by the vendor. So -- anyway, the person who asked me about that, I told them they were given inaccurate information, and I calculated everything out from the USB bus speed, which is the wires that allow the transfer, the type of compact flash, and I used the very lowest possible grade; so I've looked at several things like that.

Q Okay. But for your testimony today, you're relying on your review of the databases not those other components?

A Yes.

Q And you mentioned the hash values of those. Did the Dominion software generate a hash value for those databases that you relied on or did the initial hash value come from somewhere else?

A There are SHA files in those folders with the files.

Q And it's your understanding that those SHA hash files were generated by the election management system to travel along with the databases.

A Yes. And their technical data package has reference to that. It's part of the system check that they do when they get it so they ensure that, hey, this is coming from where I think it's from, and then they decrypt the file. In Georgia, since they're Dominion, they use compact flash, and on those tabulators when their compact flash gets inserted there's that check, and then it moves the files, and then it decrypts it. And that's how it knows it's legitimate. That's why if you have those keys you can put illegitimate data in it to include ballot images, the CVR, and you can make it seem legitimate, and the system will take it as valid votes when it should not.

Q And so then before you did your analysis of the databases you ran your own hash value and compared it to the one that was in the technical package?

A The very first thing I do when I get files is to create the hash.

Q And those matched, right?

A Yes.

Q Now you mentioned, too, I believe, and I may not have heard this right, you loaded the files into I believe you said a Dominion system?

A Yes.

Q And what Dominion system was that?

A That was for Mesa, Colorado.

Q Did you have access to the Dominion system

from Coffee County, Georgia.

A No, I did not.

Q And so you loaded the Georgia files into the Mesa, Colorado file, and do you know what version of Dominion's software is used in Mesa, Colorado?

A Yes.

Q And what is it?

A It's 5.10, but the SQL server is the same version.

Q And so the demonstration you did for the court earlier you were in a Microsoft SQL Suite of some sort --

A Studio Manager.

Q Studio Manager, thank you.

But you performed your analysis in the Dominion system or did you perform your analysis in the SQL system?

A The SQL system is in the Dominion system. The Dominion system runs a SQL server, 2016, and in that server is where the databases get loaded. In different areas in different states you'll see old databases, you'll see new databases, it all depends how the county and state runs their elections and how they preserve the data.

Q But just so we're clear for the record, in

terms of your analysis, did you use the SQL database functions of the Dominion system from Mesa --

A Yes.

Q -- to conduct your analysis?

A It's the same database server. Basic software deployment development, it's version controlled -- it's the same -- the SQL server is the same server.

Q You also mentioned I believe in your testimony you had some database experts who helped you.

Who were those individuals?

A I'm not going to disclose that.

Q Those individuals assisted you in your analysis of these databases in Georgia?

A No, not the Georgia databases. It's -- again, it's the same database structure, the same stored procedures.

Q Okay. And just so I'm clear, the individuals you referenced who were database experts who helped you were not involved in the review of the Georgia databases you're testifying about today?

A That's correct.

Q Thank you.

Now, let's talk a little bit about things

you're not offering opinions about. I believe you said you're not a lawyer, you're not offering opinions on the legal compliance aspects of Georgia's voting system, right?

A   No.

Q   And you're not offering opinions about the overall security of the system because you haven't looked at all the different components of how Georgia handles its election processes, right?

A   If the system itself is bad -- and again, if you're relying on physical security -- the other processes are irrelevant.

Q   So it's your belief then that any other element of the system does not matter from a security perspective if the vulnerabilities you've identified exist?

A   I will tell you, as I told a county commissioner in Colorado when he told me all the steps he did, and I told him you served your community well, because of everything he did, but then I put my hand on his shoulder and said, but all of it is irrelevant because the system is flawed and has no security, no integrity whatsoever.

Q   Was that also a Dominion system you were referring to?

A Yes, it was.

Q And you did not offer an opinion at all about the degree of risk, because you've concluded the system is just insecure, right?

A That is correct. If you would like a risk analysis and assessment, I would be glad to do one for the whole state of Georgia. I would ask if you have the program. If you do not have a risk analysis assessment program at work, I can do it. I helped design the one that the Missile Defense Agency uses several years back and Health & Human Services, as well.

Q And you don't have any specialized knowledge or experience about the administration of elections separate from the voting systems; is that right?

A The way the Voting System Test Labs function is they set up the different scenarios specifically if it's a state certification, which is different, because Georgia did follow federal, so they run it through the whole gamut.

So they have to set the components up in the different configurations that are listed in the technical data package, they run an election to include conducting an L&A test and then they run sample ballots through like a regular election.

Q And you participated in those processes?

A I've observed them. In certain security functions I would get to participate in them because we would look at things, especially when the vendor would try to connect something to the internet and have a fire wall that we get inundated within a minute; but yes.

Q And it's your understanding that Georgia Dominion equipment is not connected to the internet, right?

A That's incorrect.

Q So you believe Dominion voting system components in Georgia are connected --

A From unrelated Dominion documentation I can specifically tell you that there was -- there is connection.

Q Which county in Georgia was there a connection to the internet of Dominion equipment?

A It would be Gwinnett, if I'm remembering correctly. There were several states involved.

Q And which time period are you referring to?

A This was 2020.

Q Before or after the election?

A During the election.

Q And you've never participated in the training of poll workers for an election, right?

A No. I've talked to them in my home state because the training is often done by the vendors, the majority, and they asked me questions because they found flaws in the systems.

Q But you don't know who conducts poll worker training in Georgia, right?

A No, not poll worker training in Georgia.

Q Now, I understand that you don't believe physical security matters in this context?

A I did not say it doesn't matter. I said you cannot rely on it solely.

Q And you're aware that there are state election board rules regarding physical security, correct?

A True. Again, bad guys don't follow the rules.

Q And are you -- do some of those rules prohibit connecting Dominion equipment to the internet?

A I am going to get away from using the term "internet." I'm going to say network connectivity. I've noticed that many states violate their network connectivity. Their laws say no network connectivity anyway. Local Area Network still increases your attack vectors by a thousandfold.

For example, the switches, are they solely for that or are they connected to any other part of the county? It's been the case -- a lot of counties don't want to provide that information. In Arizona they wouldn't provide that data. This is the digital evidence that would show that they are -- have outbound connections, and not necessarily the internet. Some people will say it's a secure VPN, if you're in Wisconsin or Arizona, which is irrelevant, because VPNs can be had, as well.

Q So it's fair to say states have a variety of practices involving how to handle network connectivity?

A Yes.

Q Do you know if the SEB rules in Georgia require secure physical storage of equipment?

A Yes, I believe they do.

Q And do you know if those rules require limited access of who can access the equipment?

A I'm not -- I don't know all the details on that, but then again, any logging access to those systems, any of the security seal tape logs, all that should be publicly available.

For example, my company, when the federal government comes in and inspects us, there's an agency called DCSA, Defense Counterintelligence Service [sic] Agency, they come in and audit us. We provide everything to them to include our corporate information, because it's in our corporate building. That's why they have authority over us. Why? Because we're in contract with the federal government.

So every access log, everybody that badges in -- and I work in a closed area, a classified area, all that stuff is publicly available -- well, to them. And anyone, as far as the county, should be able to look at that. There's nothing classified about it.

Q And in preparing your testimony today, you didn't consider the SEB rules related to voting equipment; is that correct?

A Again, when you're talking about systems that are this bad it's a minor point on what the rules are.

Q So that would be a yes, you didn't consider that?

A No.

Q Let me ask a couple questions about your illustrative examples that you played earlier. So

you -- so the first one we talked about the password, and then you were able to decrypt and obtain the password using the decryption tool and show that the password was the same as it had previously been.

Do you recall that?

A The very first video was actually a hash of the dvscorp08!, yes.

Q And that showed where the password was similar to what it had been in the past?

A It was the exact same thing. It was the same thing I saw back in the labs back in 2008, '09, '10.

Q Do you know if the full database and those administrative account records exist on every component of the system or only on the EMS?

A For the database server?

Q Yes.

A Those -- there's an SQL lot database that goes onto the tabulators. I have not seen detailed system logs from the tabulators in Georgia, but I would find that they are not logging, just like the EMS. But specifically we were talking about the database that resides on the EMS. As for those files, they were the normal election management database, not the SQL lot versions that run on the tabulators.

Q Right. Just so we're all clear on the different pieces, the part we were looking at on the videos was the election management server that stays at the county office, not the other components of the system that are distributed on election day, right?

A That's correct. But with those keys that's easily manipulated. Like I said, I can decrypt the configuration files, and the tabulator will assume that they're legitimate, and then whatever configuration I put on the machine will run.

Q One of the other videos you showed, showed a modification of votes that you did by running some script within the database.

Do you recall that?

A Yes.

Q And the manipulation that you showed there occurred in this example after the election was over, right?

A That's because that's the way my demo went. This could easily be put on beforehand. And if you want to talk about beforehand, we can talk about supply chain management, and I could tell you some of the atrocious stuff I've seen in technical data packages as far as where they get their parts.

Q But for the specific video you showed, in

that situation, if that manipulation were to occur, we would still have the paper ballots to go back and count those, correct?

A Are you going to hand count the paper ballots? Because here's the thing that I've noticed, even if, like, the state of Florida which has -- they say they do a hand count, but they use an automated system. It's another machine. Anybody that knows anything about system testing knows you will not use the same device, or the same type of device, you will use a totally different method.

And two, it's not independent, because it has to use a ballot definition, so you've got your other third-party verifying app talking to the vendor, so it's not actually what we refer to as IV&V, independent verification and validation. So if you're not hand counting them, that's irrelevant.

And I might add I think there's a county in Georgia that's not obeying the court by providing the paper ballots to someone who requested them and won their case.

Q So -- just so I understand then, it's your view that hand counting the ballots is the only way to accurately tabulate an election?

A That is not what I said. I said when you verify it, you do it by a separate method. If you're going to audit something and do it, that's the way you perform the test, and that's the way you can do it.

I have personally went through hand counting class and observed it, and especially from my -- my major in computer science is on system design, and so you look at systems and processes, and I will state I'm pretty good at it, because I do process improvements, and that's when I've gotten financial rewards from my companies.

And what I want to tell you as far as that is that in the process it's got to be scalable, and you have to be able to adapt it, because each county -- just like each county in Georgia is different. Telfair is a lot smaller than DeKalb or Fulton County, correct? Therefore it would be a different type of a method. The main thing you want is the process to be solid in its performance, to be auditable, and that's what can be done, and it can be done accurate. The training I went through we had -- actually had a ballot with 25 races on it.

Q And you would agree that using a risk limiting audit post-election is a good practice, right?

A Only if the risk limiting audit is a valid audit, and it does not -- what I will tell you in every state or county that I've evaluated the risk limiting audit, it's been ineffective.

For a point of reference, St. Charles County, Missouri stood there -- their county official and they're over 100 percent correct on audit -- 100 percent, up and down. Sat down with pencil and paper, did the math, they did .004 percent of the votes cast in that. So what does that mean? I have a 99.996 percent of not getting caught. It's ineffective. You want your audit to be statistically significant to give you the comfort of trust that it's supposed to be. I have yet to see a risk limiting audit that does that.

Q Just so I understand then, it's your testimony that a risk limiting audit could be used to verify results of an election but the ones you've seen, like used in Georgia, do not?

A I would not use a risk limiting audit to verify. I would use a separate, totally different counting method, complete and in its entirety, because my observations -- and not necessarily in Georgia, but in other states -- I've seen more things happen during primaries and local elections, and again, counties run the election.

Q Now, when you were at Pro V&V you conducted a security review of the Dominion 5.0 system, right?

A Yes, I did several different vendors with them.

Q Do you recall if encryption keys were stored in clear text on that system?

A From 2008 at Wyle Labs where Jack Cobb, the owner of Pro V&V worked as the supervisor lead, I have not been able to do security testing to the realm that they should have been, so they were never, ever checked.

Here's the thing, the labs probably never look at them. I'll state it the way I've stated before, I felt like I had a choker chain on me from Day 1 in those labs. They do not test these systems to the appropriate level they should be. What they do do, is the lab will spend a week getting the big tabulators -- like for ES&S the 859, the DS850, big monster machine that they have to spend a week to configure to get it to pass the certification test, or you talk about the ICCs. The labs will spend more time getting them to pass certification on that portion than they do on security testing.

Q So the -- your testimony then is while you

conducted some testing on the Dominion 5.0 system, you don't know if the encryption keys were stored in plain text because you never looked?

A I would be -- only -- I would be allowed to have, like, one, two -- maybe three tests, because you have to do up a test, right -- in basic system development you have use cases and your requirements and that's how you develop the system. Then you go in and test it, and in the test there's a part, of course, that would be security.

And so I would write up my test cases -- here's the thing I would tell you: In earlier Dominion systems, like 4.14 -- I've done several of them -- I would do a test, it would fail. I would want to redo the test in the new version, and I would be told, no, you've already done it. And I'd say, but it failed. And they go, no, do something different.

Again, why I stopped, I got tired of the rubber stamping, and it was typical federal agency type stuff with the EAC. Just boom, boom, boom, no matter what I put in my internal security report to the lab, they always got certified either by a state Secretary of State or by the EAC.

Q So it's not your testimony that the lab was doing something inconsistent with the EAC, it just

wasn't doing as much as you thought needed to be done to test the security of the system, right?

A They -- well, because you'll pull me to hearsay -- I will tell you that states are supposed to be, just like in Georgia, where the Secretary of State has the final say, even though it's supposed to be federally certified, when it came to the labs they would say, well, it's got to go through a federal lab, so we've got to do all the tests, but it's state certification, so we don't care; so are you going to allow that? I can tell you who said it and the multiple times he said it.

Q Now, you are aware that the federal CISA -- I can't remember all the acronyms.

A C-I-S-A, yes. I'm very familiar. I've talked to several of them -- southeast region.

Q So CISA is a federal agency involving infrastructure or security.

Would that be a fair statement?

A Yes.

Q And you're aware they reviewed Dr. Halderman's report in the Curling case, right?

A Yes.

Q And they issued recommendations around security practices for Dominion Voting Systems after

reviewing that report, right?

A Yes.

Q And I think we said earlier the encryption key issue was contained in Dr. Halderman's report, right?

A What you're trying to infer is out of the eight things that they listed that were very limited in scope didn't cover half of what Dr. Halderman covered.

What I will tell you is I know, because I talked to the southeast region -- Georgia falls in the same area as Alabama -- for many years. See, I attend forensic conferences, usually in Myrtle Beach, South Carolina because of the environment, right? Can't blame you.

So as I attend that, they had one representative. There are three gentlemen now that handle the southeast region. So when you look at that, and CISA is also responsible for providing recommendations to industry within those regions to the municipal governments, for example, city and county infrastructure. If you don't want -- as Fulton County got hacked and everything went down, if you don't want that, you're supposed to consult with them, and some of their people are pretty good.

What I will tell you is, is their evaluation of Dr. Halderman's report was probably very limited and very rushed to put something out to the public because his report was going to be public.

Q And so you'd agree with me then that the encryption key issues you're flagging in this case were not part of CISA's recommendations after reviewing Dr. Halderman's report, right?

A They missed a lot of stuff.

Q But those -- CISA made no recommendations about encryption keys after reviewing Dr. Halderman's report, right?

A That's true. It wasn't in the report.

Q If I could have just a moment, Your Honor.

Just a couple more questions.

I asked you earlier about the 2024 election results or whether people could trust those results. Is it your testimony that Georgia voters can't trust the results of the 2022 general election held in Georgia?

A I would say yes.

Q Is it your testimony that Georgia voters can't trust the 2024 general primary results held in Georgia?

A Considering the state of these systems, yes.

MR. TYSON: That's all the questions I have, Your Honor.

THE COURT: Any redirect?

FURTHER EXAMINATION

BY MR. MacDOUGALD:

Q If you could go to Tab Number 19 and turn to Section 8.

What is the title of Section 8?

A Give me just another second.

Q Yes, sir.

A The title of Chapter 8 is Quality Assurance Requirements.

Q All right, sir. If you would please direct your attention to Section 8.1?

A Yes.

Q And that first paragraph, if you would please read into -- read to the court the first two sentences.

A "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 the system development and continues throughout the maintenance life cycle of the voting system."

Q And so that means -- while it's being used in elections?

A When you talk about the maintenance life cycle of any system, that's from inception to death. So if you get a new system, you start tracking it, you analyze it, you maintain it, you record all those.

We have a system that we use with our program that everything -- when it comes in from procurement, it's in the system, there's change requests done on it -- everything that's done with that system is tracked until we decommission it.

Q All right, sir. And you were asked questions about whether software updates would require a new certification.

Do you recall that?

A Yes.

Q Are you aware of whether the Dominion system has applied Windows security patches and updates since it's deployment?

A No, I'm not. I've seen a couple of them with ES&S, but that's something that doesn't go -- to further this point, I have voiced my opinions to the lab when I was in them that when you bring a new system in and you're going to get it certified for use and sell the product, you would bring -- you would agree that you would bring your best, that you would make sure everything functions, that we've tested it internally and it's good.

I've been in the lab and seen antivirus in the certification lab now, not even being used, so we're not even talking about having to update it yet -- two years. Two years, the definitions are out of date. The version -- the antivirus actual application, is several years behind with multiple vulnerabilities in it, and this is just talking about the antivirus, and that's was what was delivered in certification, let alone maintaining. But as far as engineering change orders and normal patch management processes that the rest of their industries -- anywhere that deal with IT, no.

Q So to your knowledge, are security updates being applied to the Dominion systems used in Georgia?

A No, they're not. I wouldn't see all the vulnerabilities I do. You can pull any test report from the EAC site, all you have to do is type in Google, CVE and that software listing and the version number and I guarantee you'll find multiple vulnerabilities of high and critical.

Q Do you have any understanding of why the

state of Georgia -- well, let me back it up.

Do you have any understanding of why these systems in Georgia have not been updated with those security patches?

A No, I do not.

Q From a security standpoint how would you characterize that practice?

A That's gross negligence.

Q You were asked a number of questions about the keys being different from one county to the next. Is that true with respect to the X.509 certificates?

A No, they're the same.

Q And they're not just the same from county to county, they're the same from state to state that you've examined?

A Yes.

Q All right. And the same question for that vendor password, dvscorp08!, is that different for every county?

A No.

Q Is that different from state to state?

A No.

Q And how long has it been the same on all the Dominion systems?

A I saw it in the test labs, and like it's documented by the EAC even as a deficiency, so it went forward formally in 2010, but I know I've seen it prior to that.

Q And the vendor password, if employed, gives a user what authority on the system?

A Yes, they would have administrative access. Here's the thing, these systems are so horrible any access to the system -- there are so many vulnerabilities where you can escalate your privileges, so even the normal user who wouldn't have it as they're working could just exploit one component of that system and elevate their privileges and then act like they're an admin.

Q And you talk about escalating privileges, elevating privileges, that sounds like an industry term.

What does that mean and how is that type of thing exploited, if it is?

A So in normal organizations you're going to restrict users' access. We call them privileged users on the program I work at, and even those are admins. They get -- there's special access that you can have to run applications, because some applications require system-level or what we refer to as root access.

When those applications do -- if they have a vulnerability and you're allowed to run them, you can exploit them, and you can raise from your limited access -- for example, the probate judge that allowed me to look at a system in Alabama -- he got a little too afraid and wouldn't let me touch -- but I had him log in, and his limited visibility as we looked at the systems -- and that's how I came to the 300-and-something vulnerabilities -- he could have easily, on just the access he had, manipulated -- run the script that he copied down from Google, or one of the hacking websites, ran it, and been -- elevated his privileges up and become admin and seen things he couldn't normally see.

For example, a lot of the vendors will not let you see that the wireless connection is on, and you won't be limited, you can't do that. On my program, because classified systems have to be up 24/7, normal users can't shut them down. When you go to hit the power shutdown button, you're not authorized to do that. It tells you that. You give levels of access to what they're doing.

Q   In the configuration of these Georgia election systems that we've been discussing, are they robust to nation state threats that are faced by the United States?

A No. No, they're not.

Q And how would you characterize the level of capability of the adversary compared to the level of protection in these systems?

A Considering nation states like China have buildings, literally, with people that probably make me look silly as far as my technical capabilities, it's a cake walk.

Again, I say someone of Kiddie Scripter Level 5 that watches a few YouTube videos and can understand the basics of a computer can manipulate these systems easily.

Q Now, you were asked a few questions about air gapping or internet connectivity, and then you express it in terms of network connectivity.

Just to be clear, is the air gap that's touted in this system actually an air gap, and is it -- does it protect the system against penetration?

A There are different areas -- and this is only an argument depending on what state you're in because how they define the system and the voting system. To me, as a security person, you have to look holistically. Me, as somebody who has hacked before, you look at the whole system, because there are things in the hacking world called pivot points.

For example, if I can get in on the poll book, then that means I can get to the printer if they have the ballot-on-demand printers like a lot of states do. I can manipulate that. I can insert a QR code on that that could execute some malware on the tabulator. There are literally thousands of ways to do it.

I see some states that actually violate their law, because they say no capability, and yet the systems have capability. There's not -- there's probably not an EMS out there that doesn't have a wireless or a bluetooth card on it, and I'm keeping it simple, because you don't need those cards on there to manipulate and to establish a communication channel. Those are the primary ones that normal people understand.

Q   Despite the air gapping?

A   Despite the air gap. And again, air gap systems can -- and they'll use this term -- it can include network connections, but the minute you have network connections you increase your attack vectors a thousandfold.

And what I will say is these air gap systems utilize compact flash, USBs, removable storage. I can tell you I put files, they were harmless, but I put files on Dominion and ES&S systems, and they did not identify them.

Q Through the path of removable media?

A Yes, on that, and on the systems to where they actually had the data encrypted as it should be, what I've noticed during forensic examinations is a lot of this election data is not encrypted.

For example, I can't remember the Georgia county, but when they removed the compact flash or USBs during the election and replaced them for some reason, that would leave that data that was currently on there in an unencrypted state. That does not happen until you close that tabulator -- until you close that poll down on that tabulator.

Q And so the removable media, when they go in and out of the slots from one machine -- one component of the system to another component of the system, that's mechanically bridging the air gap?

A Yes, sir. And another thing as far as that is the election not reporting. Right? When you've got your main reporting server, usually on an EMS, and it's air gapped, but yet if they reuse that -- and that's where procedures come into play, because some don't. If they reuse that USB and take it to the internet-connected computer and transfer that data off to the other third-party private entities that probably shouldn't be involved in elections, when that gets done and then they plug it back in, was there any virus -- oh, we're going to check with the two-year-old virus definitions that have never been updated? And virus definitions are irrelevant to any good hacker anyway -- but the thing is there's no check on the integrity of that USB and that compact flash that gets transferred back and forth.

Q Between the internet-connected machine and the server?

A Yes, sir.

Q So are we talking about a Tom Cruise Mission Impossible-level terms of difficulty to get across the air gap?

A No, no.

Q All right. Okay. To your understanding is Dominion able to remotely connect to these election systems?

A Yes.

Q Are they able to do that without detection?

A Yes.

Q And are you aware of any instances in

which that has occurred?

A Yes.

Q Can you identify those instances?

A One would be the Denver, Colorado server was granted, or requested to grant, Belgrade -- only Belgrade. I did search. There is a Belgrade, Montana. Again, why would Montana need to connect into a Colorado file transfer server as part of the election system?

And there were other components and things that were done in the background concerning the database and the configure of the database server that still do not have an engineering change order. Because as somebody who works in operational environments for a lot of different things, what I will tell you is sometimes things break or you have a problem, and you have to fix it, and you submit a change request -- or in this case an engineering change order, that is retroactive. You want it go back and make sure that you record the process so that you have change management and integrity of the system. If you do not record changes you lead yourself down a very bad road.

Q All right, sir. Does the storage and management of the encryption keys relate to or affect

usability of the system?

A To the user and the way the system functions, no. If your question is would voters be affected? Would county workers be affected? No, they would not.

If I might state something on hard disk encryption, because I suggested that from 2008, on, every year. I would listen to these software developers tell me how it was going to be a hit on performance on the election systems. These election systems are nothing but a database server that's taking in data and adding the data and printing reports.

We run classified systems, and everything has disc encryption. So I dealt with that now, finally once some videos have gotten out of how easy they are to get in, they're trying to implement changes like that. So as far as those systems and the way they design it and the functionality or affecting a voter, no.

Q All right, sir.

A It's underneath. It's behind the scenes.

Q Thank you.

Now, the common vendor password that we talked about dvscorp08!, does that relate to or affect

the user experience usability?

A No.

Q The -- you have stated your opinion a couple of times in response to my questions about whether the system complied with the VVSG guidelines.

Was that a technical opinion or a legal opinion?

A That was my technical, professional opinion.

Q All right, sir.

A Now, I do know enough about contract law that when certain sections say "shall" and -- you don't violate it. So if you shall do a requirement, and you don't do the requirement, I don't see how that gets to be into a legal basis. You did not follow it. It's either a yes or a no, and the way I read it, it's binary.

Q All right, sir. Now, the -- you mentioned that certain components of the system are connected to a local area network?

A Yes, usually your ICCs are connected, and they report back that way. And then you have -- you have what's called adjudication work stations -- there's different levels. Each technical data package from the vendor, they'll give different designs --

again, because each county is a different size. You may not need all the components of that system, so they provide different configurations, and each of those configurations are supposed to be tested.

Q And the X.509 certificate that we've talked about, that's how one machine on a network knows to trust another machine on the network?

A Yes, sir.

Q And so the X.509, the presence of that on the system, is designed to enable network communication; is that right?

A Yes.

Q So now Professor Halderman's report, if you would please turn to Tab 21 -- Tab 21.

A (Complies.)

Q Does that report identify the system component that he was analyzing?

A On the front cover page?

Q Yes, sir.

A It says it's for Georgia, and it was that ImageCast -- it's the ImageCast X Ballot Marking Device.

Q And is that the election server or is it something else?

A That's a ballot marking device. It's for accessibility for those with disabilities. And what you do is you mark your ballot on the screen, and then it prints a ballot. Which I might add, and I will state this, because I know the VVSG requirements. Title III, Section 301, Paragraph A, the voter will verify in secret, in confidentiality or something like that, their ballot is correct before they cast it.

There is no human being that can read a bar code or a QR code and verify their vote. I dealt with a hearing in Pennsylvania where the printed text at the bottom, which is not evaluated by the system, was different than the bar codes. These were ES&S systems, and people complained, and they allowed it on a clerical error.

The clerical error that the court dismissed everything on there is a technical flaw in the system that should be that, and to my professional opinion, based on what HAVA requirements are, that these systems, whether ES&S or that -- if they use a bar code or a QR code, they're in violation of the HAVA.

Q All right, sir. Now, I would like for you to turn to Page 48 of Exhibit 21, the Halderman report, and let me know when you're there.

Are you there?

A Yes, sir.

Q Do you see the indented line towards the bottom?

A Yes, sir.

Q Does that look familiar to you?

A Yes, it does.

Q And what database -- well, tell me what that is and what database is being queried?

MR. TYSON: Your Honor, I'll just object at this point. We don't have this in evidence, and so I think this is getting a little squirrely in terms of how we're handling this.

THE COURT: Mr. MacDougald, what's the ultimate point here, if it's not for the truth of the matter asserted?

MR. MacDOUGALD: This is in rebuttal of questioning on cross that the database with the encryption keys vulnerability existed only on the server, and this report demonstrates otherwise, and I'm calling it to his attention.

MR. TYSON: Your Honor, I will say that wasn't the testimony, I don't believe. I believe the testimony was there's a SQL light database that's on the DMD versus the entire database.

THE COURT: Regardless, wouldn't that -- you're now doing exactly what you said you would be unable to do, which is to say that whoever wrote this report, you're now putting it in for the truth of what's in the report?

MR. MacDOUGALD: I'll ask him if he has independent knowledge.

BY MR. MacDOUGALD:

Q Do you have independent knowledge of whether the encryption keys are stored in plain text on the ballot marking device?

A Yes. They're the secret, private keys and they're -- obviously this is the same exact query.

Q And how do you know that they're -- apart from Halderman's report, do you know that?

A Because these Rijndael encryption keys are symmetric. There's two different types of encryption. There's symmetric and there's asymmetric. And that's the reason they're a private key and they're supposed to be stored securely, not in plain text, is because if you get the key you now risk exposure.

They're a lot faster to authenticate and they're used, but usually -- and we'll talk server communications and authentication. You authenticate with asymmetric, right -- public, private certs, that's quicker, you get the connection, and then you exchange the private key, and these are considered private keys, and they're sitting on the tabulators -- this ICX and this one.

Q Do you know that apart from the Halderman report?

A As actually having an ICX image, myself? No.

Q So how do you know it?

A Because the queries here and the way the components are built and designed, they have to. It's just the technological piece of it.

Q In order for the ballot marking devices to work as a part of the --

A How would the tabulator decrypt the DVD configuration files and operate it if it couldn't decrypt the encryption? It's basics.

Q In order to do that, it has to have the same encryption keys?

A Yes, because of the way this is, yes.

Q And those encryption keys that were used to encrypt those files, that was done on a --

A The same key and the same vector are on the tabulators, the other components.

Q All right. You mentioned supply chain.

Help the court to understand what the concept of supply chain vulnerability is.

A Well, considering Lockeed Martin made me go through the class on this, I'll try to keep it short for the court. But especially specifically in any major company where you were worried about -- especially in a DOD environment, a weapon system, information system -- whatever the case is, you want to know that from the concept of the products used to build your components is done in a secure manner because technology today, you can fit a microprocessor on the tip of your finger and barely be -- it will look like a speck of rice, even smaller, and these things are that. I know -- Northrup Grumman tauts it on their website.

And the thing with these types of things, it can be embedded. Years ago there was a USB battery charger that they did not discover that China had malware on it until ten years after the fact. It had already went off market before -- so how many computer systems, how many people's systems were infected with that? And that's why you have to look at the products, where they come from. It's called global supply chain, and you go through that management. And certain companies have the training products, and it's so you ensure the products and the components that you use to assemble your system are secure.

Q   And the system, the election systems that are used in Georgia, do they -- do you know anything about their supply chain? You mentioned it in response to Mr. Tyson's questions.

What can you tell us about that?

A   I cannot speak -- I have not seen the 5.5A technical data package. I will tell you I've seen several other technical data packages, and to that fact some of these components that are in the newer versions are the same components that are in the older versions.

Q   And you're talking about hardware components?

A   Yes, sir.

And so because these tabulators are basically optical scanners with some other homegrown software thrown on them and other components, certain kind of a little small printer to print reports and do the things it needs to do. You have to have separate -- in the bins you're supposed to separate stuff that goes into the adjudication database to go to a different one, and all that, so there's a lot of mechanical points that they build these things.

I will say some of them are built poorly, because they're supposed to run off backup battery in case you lose power. As they found out in Arizona, you've got to plug them in 20 minutes before you can even power them back on or they'll stop charging. That's poor system design.

And so -- anyway, these components have to be listed in the technical data package. What I can tell you I personally verified is that there are same e-mail addresses for components that go from different countries and then there's bogus ones, and it's laughable at what they consider supply chain management as far as voting systems.

MR. MacDOUGALD: That's all the questions I have.

THE COURT: Any recross on those points?

MR. TYSON: Just briefly, Your Honor.

FURTHER EXAMINATION

BY MR. TYSON:

Q I'm going to follow up on a few of Mr. MacDougald's questions. First of all, as I understood your testimony, it's your belief that any ballot marking device system that's used for all voters that uses a barcode or a QR code, it either is or should be illegal; is that right?

A Yes.

Q And so there's no configuration of Georgia's Dominion system, if it prints a QR code, that you would consider to be compliant with law and structures involving voting systems, right?

A As far as with the voter being able to independently verify.

Q Mr. MacDougald asked you about system updates. Do you recall that?

A Yes.

Q You would agree with me that Dr. Halderman covered system vulnerability in his report in the Curling trial, right -- system update vulnerabilities?

A Yes.

Q And he also covered privileges escalation as part of his report?

A Yes.

Q And he also covered root access in his report?

A Yes.

Q He also covered nation state threats faced by the United States and the states?

A Yes, as far as ease, I believe, of access -- getting into the systems.

Q When Mr. MacDougald asked you about

internet connectivity, you mentioned you put some files onto Dominion systems.

Did I get that right?

A Yes.

Q And you did that in your lab environment at the Voting System Test Lab, right?

A Yes.

Q Mr. MacDougald asked you about the air gap and moving election results from the EMS over to the election night reporting computer for each county.

You have not reviewed the training that is provided to county election officials about how to do those uploads, right?

A Specifically to Georgia, no.

Q You also mentioned Dominion remotely connecting to election systems, but you don't have any evidence that occurred in Georgia, correct?

A There was one county. I've seen a lot of Dominion e-mails. I've had to translate Dominion e-mails from Serbian to English to verify the technical questions I was being asked about them, to verify that it was translated properly, so --

Q So it's your testimony that there is evidence of Dominion remotely accessing Georgia election equipment?

A Yes, on the one county. It was included with stuff that I was researching and reading through considering Colorado. Michigan was also involved, and there were other ones.

Q So I'm focused specifically on Georgia, and we're referencing the Gwinnett County 2020 incident.

Is that what you're referring to?

A I believe so. I have went through a lot of Dominion e-mails.

Q And ultimately for all the different vulnerabilities we're talking about, someone has to gain access to the system in some way, right?

A Yes, either locally or remotely.

Q And I believe earlier we covered that of all these different vulnerabilities that every voting system has vulnerabilities, right?

A Every system has vulnerabilities. The thing is that these voting systems -- irrespective of the vendor, have a ton more. I don't take that saying your home PC is more secure lightly. I'm a professional with over 20 years experience in this field. I have worked in every federal agency there is, I've been consulted by private companies. I've worked internationally for NATO, recovered NATO's infrastructure when it was being rebuilt and had an issue, so I do not state that lightly. These systems are horrible.

Q   And you'd agree that ultimately each state has to decide which vulnerabilities it wants to encounter when it's choosing an election system, right?

A   That's basic risk management, and that resides even outside of technology areas. There's all kind of risk assessment and analysis when there's risk. Anybody that deals with a contract knows this.

Q   But ultimately it's up to the state to make that selection of that voting system, right?

A   Yes.

MR. TYSON: That's all the questions I have, Your Honor.

THE COURT: All right. Mr. MacDougald, can this witness be excused?

MR. MacDOUGALD: He may, Your Honor.

THE COURT: Okay. All right. Thank you, sir. Please step down.

All right. You may call your next witness.

MR. MacDOUGALD: I call Ben Cotton to the stand.

(Witness sworn.)

WHEREUPON:

BEN COTTON,

having been first duly sworn, was examined and testified as follows:

EXAMINATION

BAILIFF: Will you state and spell your first and last name for the court?

THE WITNESS: My name is Benjamin, B-E-N-J-A-M-I-N, Cotton, C-O-T-T-O-N.

BY MR. MacDOUGALD:

Q All right. Mr. Cotton, where do you live?

A I live in Big Fork, Montana.

Q How are you employed?

A Well, until this last Friday I was the vice president for incident response for eSentire, USA. I retired from that position. As you may be aware, incident response is a 24/7/365 commitment, and my wife was diagnosed with a medical condition that requires someone to care for her.

Q So you mentioned incident response. What does that mean?

A Incident response is the industry term for responding to a crisis in which a hacker has penetrated a network and is exploiting that network, whether it be for personal gain, monetary gain or just kicks and giggles.

Q And so that's IRT. Is there something called HIRT?

A The HIRT program, H-I-R-T is -- it stands for Hunting and Incident Response Team and that is a subdivision of the CISA -- DHS CISA agency, and I have supported that as an active member.

Q All right. So the hunting part is what?

A The hunting is actually looking for finding out who did the penetrations, looking for these breaches, and then trying to perform an [unintelligible] to those intrusions.

Q All right, sir. Prior to your last employment, I can't remember the name or pronounce it correctly, what did you do?

A So I basically got into computer forensics through the military. I'm a 21-year veteran of the military, of the Army. 19 years of that was spent within the Army Special Operations Command. The last six years of that was spent in support of a special mission unit as a fully-qualified operator.

As part of that military service I got involved in what myself and two other people for that special mission unit termed digital media exploitation. And that is essentially exploiting devices we found on the battlefield and turning that into actionable intelligence to feed the operations and intelligence sector. In 2003, I retired --

Q From the military?

A -- from the military, and I became a civilian contractor for the Drug Enforcement Agency as a senior forensic examiner in the digital forensics lab in Norton, Virginia for the DEA. I subsequently moved, or was asked to join an effort that performed the deep dive computer forensics for the high-value terrorist target disk drives that were seized overseas as part of the CIA.

Q Was that for -- in connection with the Gulf War or was it generally post-9-11 work?

A That was post-9-11 work. Basically from the beginning of 2004 through 2007 I was part of the team that did all those deep forensics examinations.

Q So after you -- so then what? Take me up to eSentire.

A So I created a company called Cyber Technology Services. We did business as CyTech Services. We supported the intelligence community, other government agencies, both from analytic and digital forensics support up through that time period.

Additionally, when I retired from the military, I was hired by Guidance Software. They were subsequently acquired by OpenText, O-P-E-N-T-E-X-T, and I was the instructor for the EnCase forensic software, so I taught other experts how to use the EnCase software.

Q And what is the EnCase software?

A The EnCase software is a GUI-based analytical platform that will perform forensics imaging and it will also conduct detailed analysis and allow the examiner to conduct detailed analysis of forensic images of digital media that is pertinent to law enforcement, intelligence, or whatever the issue may be.

Q That's a standard tool in the business?

A It is.

Q All right, sir. So you formed this company called CyTech?

A Yes, sir.

Q Did you remain at CyTech all the way to --

A To eSentire.

Q -- eSentire?

A No, I did not. So as part of the CyTech experience we actually created our own digital forensics software design for very large enterprises.

And essentially, if you're familiar with computer forensics, then you've ran into one examiner, one computer dynamic where it's very difficult to analyze or triage tens or hundreds of thousands of computers at once. Our software was created so that we could perform forensic analysis across hundreds of thousands of computers simultaneously and return results in the same amount of time it would take to examine one computer. That software, we spun it off into its own company in 2018 called CyFIR, that's C-Y-F-I-R.

Q And what was your role in the development of the CyFIR software?

A That was my brain child. And I also assisted in the development, the testing, and you know, the full spectrum as CEO of that company.

Q And then from CyFIR to eSentire?

A So eSentire actually purchased CyFIR in 2021, and they insisted that I come along as part of that deal.

Q All right, sir. Any notable achievements in the attribution of significant cyber penetrations or hacks?

A So as part of the demonstration to the office of personnel management in, I believe that was

April of 2015, we were -- we discovered the Chinese breach of OPM, which resulted in the largest breach in the history of the U.S. government, and that was attributed back to the Chinese.

Q And how long had that gone undetected, if you know?

A Almost three years.

Q Do you hold any security clearances?

A I do. I hold a top secret government security clearance.

Q Have you ever had higher levels of clearance?

A As needed per specific programs, I have been involved in multiple secret compartmentalized information for SVI programs.

Q All right, sir. Any prizes or rewards in your field?

A I don't remember the exact ones. We had multiple, you know, best technology, leading technology, that type of thing, from different magazines and industry groups.

Q All right. I believe you've got a binder on the table there with you?

A Yes.

Q If you would please turn to Tab Number 22?

A (Complies.)

I'm there.

Q You'll see a document there marked Exhibit Number 22, first page lower right corner?

A Yes, I see it.

Q Can you tell the court what that is?

A This is a copy of my CV.

MR. MacDOUGALD: All right, sir. Now, I'll tender Exhibit 22 into evidence, Your Honor?

MR. TYSON: No objection.

THE COURT: Exhibit 22 is admitted without objection.

(Exhibit A-22 was tendered and admitted into evidence.)

BY MR. MacDOUGALD:

Q All right. We've talked about your background, qualifications, training and experience. Anything else on the CV that you think is worth pointing out to the court?

A Well, I do have a masters degree in information systems management, and I hold a CISSP certification, as well.

Q All right. Any other certifications?

A I am certified investigator with the CyFIR technology, as well.

Q And do the certifications that you hold require ongoing training or updating or continuing education?

A Yes.

Q And you complete those every year?

A Yes.

Q Are you familiar with the election systems used in Georgia?

A I am.

Q How are you familiar with them?

A I was first asked to become familiar with them as a retained expert by Stefanie Lambert for her client, Misty Hampton, in Coffee County.

Q And what version of Dominion software is used in Georgia?

A Dominion Democracy Suite Version 5.5 Alpha (A).

Q In the course of your work and training and experience have you had occasion to become familiar with something called FIPS 140-2?

A Yes.

Q And how did you become familiar with that?

A Well, FIPS 140-2 is required any time a technology is going to be utilized by the federal government that contains security encryption functionality it has to be FIPS compliant. And so for our CyFIR software, we became very familiar with FIPS in the development that that software and our algorithms.

Q   So how would you characterize your familiarity with FIPS 140-2?

A   I would say that it is more advanced than the average security guy. I'm not a FIPS certification expert, but I'm certainly aware of the criteria.

Q   All right. If you would please turn to Tab 20, and tell the court whether you recognize the document marked Exhibit Number 20.

A   Yes.

Q   And what is it?

A   That is the FIPS Pub 140-2.

Q   Pub?

A   Yeah, right at the very top. It means published.

Q   It's not like an English or an Irish pub, right? It's a publication?

A   It's a publication.

Q   And it's put out by whom?

A   By NIST.

Q Who is that?

A National Institute for Science [sic] and Technology, I believe is what that stands for.

Q Standards and technology?

A Standards and technology, yes.

Q I've got you guys on acronyms today.

A There you go.

Q Given your work in cybersecurity, are you familiar with something called encryption keys?

A Yes, I am.

Q What are they?

A Encryption keys are utilized from two aspects. One is to authenticate accesses to ensure that when a system or a user is actually accessing the system that they are supposed to access it, and it's also used to encrypt and decrypt information and protect that data from unauthorized disclosure.

Q Now, are you familiar with the industry standard protocols and practices for the storage and management of encryption keys?

A I'm familiar with the requirements, yes, sir.

Q All right, sir. And are you also familiar with the U.S. Election Assistance Commission certification requirements as they relate to

encryption keys?

A I have reviewed them. I don't know that I would class myself as an expert, but I am familiar with them.

Q All right. And does FIPS 140-2 address the topic of encryption keys?

A Yes, it does.

Q And you're familiar with that.

A Yes.

Q Have you had occasion to examine the election -- you've answered this in part already, but have you had occasion to examine election databases in any Georgia counties that were used in the 2020 election?

A Yes, I have.

Q All right. Can you identify the counties that you examined?

A Yes. So Bibb, Telfair, Appling, Jones and Coffee.

Q All right, sir. Have you examined those databases with respect to the storage and management therein of encryption keys?

A I have.

Q Have you examined or analyzed what could be done by a bad actor who had possession of the

encryption for the election systems used in Georgia?

A I have.

Q Have you ever testified as an expert before?

A Yes, I have.

Q About how many times?

A I was first qualified as an expert in federal court in 2007, and between depositions and actual court appearances at least four or five expert engagements per year after that.

Q Okay. So since 2007?

A Correct.

Q Four or five a year?

A Yes.

Q All right. Have you ever been excluded as an expert due to lack of training, skill, qualifications or expertise?

A No.

Q Have you ever testified as an expert regarding any aspect of the Georgia election systems or Dominion election systems?

A Yes, I have.

Q And where have you done that?

A Specifically in Arizona. I also have provided declarations in Michigan on three separate occasions. I have provided declarations in support of the Supreme Court of Appeals in reference to Arizona, as well.

Q And what aspects did your testimony cover in those instances?

A Cybersecurity basics, the state of the systems, the state of the databases, and the vulnerability aspects of the systems.

Q Have you ever testified regarding the encryption keys and how they're stored and managed in these systems?

A By declaration and affidavit, yes.

Q And when was the first such declaration?

A Well, the first time I was aware of these encryption keys issues was in March of 2021 as part of the Antrim lawsuit. I've provided input to the declarations and affidavits at that time, and I also had provided declarations concerning these databases more recently in the Arizona case.

Q In March of this year?

A In March of this year.

Q And do you recall the first time you ever connected encryption keys to certification standards, if you ever did?

A The first time I really was asked about that was in conjunction with this case, and that would have been about a month and a half ago.

MR. MacDOUGALD: All right. Your Honor, at this point I tender Mr. Cotton as an expert on cybersecurity in general, encryption keys and how they should be stored and managed and how they are actually stored and managed in the election systems used in Georgia.

THE COURT: Mr. Tyson?

MR. TYSON: I have some voir dire, Your Honor.

VOIR DIRE EXAMINATION

BY MR. TYSON:

Q Good afternoon, Mr. Cotton. My name is Bryan Tyson. I represent the Secretary in this case.

I wanted to ask -- I believe Mr. MacDougald asked you about your testimony on the Georgia system, and you mentioned an Arizona case.

Did you talk about the Georgia system in any of your testimony in the other states that you mentioned?

A As part of my declarations I have included the Georgia analysis in the analyzed systems from a holistic perspective.

Q But you have not offered opinions specific

as to Georgia's election system in Arizona or Michigan or other states, right?

A Only to the state of the correlation of widespread vulnerabilities across the Dominion systems.

Q And your first work in cybersecurity related to voting machines happened after the 2020 election, right?

A That's correct.

Q And for your testimony today you're relying on your review of the Coffee County EMS?

Is that part of your reliance?

A In part, yes.

Q And you're also relying on the databases from the four counties that you referenced?

A Correct.

Q Have you reviewed any EMS files from any other Georgia county besides Coffee County?

A Are you talking a forensics image of those devices or are you talking just the databases?

Q A forensic image of those devices.

A Only Coffee County.

Q Did you have access to any other counties -- a forensic image of any other county's EMS in Georgia, besides Coffee?

A I did not; however, I would offer my services should the Secretary of State make those available.

Q Now, in part of forming your opinions in this case you relied on Dr. Halderman's report in the Curling case, right?

A I reviewed his report. What I'm relying on is my own analysis and findings within the scope of this case.

Q So fair to say you reviewed his report as part of your process, but you did your own analysis of the systems.

Is that a fair statement?

A That's correct.

Q Now, you don't have any specialized knowledge regarding election administration, correct?

A Only what I have gained as experience since 2020 as part of these legal proceedings.

Q And you don't have any special training or knowledge about Georgia's system apart from what you've looked at with the Coffee County system and these four databases; is that right?

A Well, unfortunately, the ability to analyze those systems is strictly controlled and some might say hidden by the restrictions put in place in

Georgia.

Q So that would be a yes to my question, then? You're relying on what you've looked at, those five items?

A I'm relying on what I've looked at as the basis of my examination.

Q And are you being paid for your work in this case.

A I am.

Q And what is your hourly rate?

A 350 an hour.

Q And when were you first hired to work on this case?

A I was first engaged for this matter -- probably the end of July I was asked to take a look at it.

MR. TYSON: Okay. So, Your Honor, we would -- don't have a dispute of Mr. Cotton testifying as to cybersecurity generally. I don't think he has a sufficient basis for specialized knowledge about the Georgia election system itself to testify as to the Georgia specific as well as the Dominion systems. We object on that basis.

THE COURT: The system including all

aspects of it, like to include the encryption keys which are the heart of the issue?

MR. TYSON: Yes, Your Honor. To include the encryption keys -- I think he can speak to encryption key storage and management, generally, but the scope, as I understood it, was specific to the Georgia election system and we would object to that.

THE COURT: All right. But it's fair to say that he's saying he's just making extrapolations based on what he learned through Coffee County. Is that --

MR. TYSON: Correct. I think that's right.

THE COURT: I'll note the objection and it's preserved for the record, but I'll overrule it and Mr. Cotton can proceed.

MR. MacDOUGALD: Thank you, Your Honor.

CONTINUED EXAMINATION

BY MR. MacDOUGALD:

Q On that point, did you examine the backup election databases from Appling, Bibb, Jones and Telfair?

A I did.

Q And so your opinion is based not just on

your examination of the Coffee County forensic image but also the files -- the backup election databases in the other four counties?

A Correct.

Q So you've examined five Georgia counties?

A Yes.

Q And have you examined any other Dominion systems anywhere else other than Georgia?

A Yes.

Q And you examined the databases in those systems, as well?

A Yes.

Q And -- okay. We'll come back to that.

Are encryption keys any part of the Dominion system used here in Georgia?

A Yes, they are.

Q How are they used in the system here?

A So they are used to authenticate systems and establish trust between one system and another, authenticate the user activities on a trusted system. They're also used to protect the data.

So, for example, in a tabulator, when you scan the ballots you are generating images of those ballots, and you are also generating a results file, .dvd, and you're generating a cast vote record as part of that. So those keys are utilized to, one, encrypt the DVD files. And any encrypted file that that system utilizes, those specific encryption keys are used to encrypt that data.

It's also used to facilitate the transmission or transport of that data, whether that be over a network or whether that be via a USB or SD card. Those encryption keys are critical to ensuring the integrity and the assurance of the voting process.

Q In light of how they are used, are they important to the security of the system?

A They're vital. It might be noted that if one takes the time to examine the certification documents that are present on the public website at the EAC, there's actually a matrix there of risk mitigation strategies from different threats, and encryption of data and the securing of transmissions is used in almost every single one of those mitigation efforts. That shows you how important it is for those keys to -- to the system.

Q If a bad actor with some skill has access to the system and access -- can they get access to the encryption keys?

A Yes.

Q And if they do that -- if they're able to

do that -- how would you characterize the overall security of that system?

A Well, in context to the voting system, they could completely manipulate and control both the reporting and the artifacts that are contained for some of the levels of the audits that are conducted by different states.

Q And how is it that access to the encryption keys would enable them to do something like that?

A So simple scenario: Let's say, for example, that the encryption keys or the voting results on the SD cards from the tabulators are being transported from the precinct to the location of the EMS. If an insider or an unauthorized person could gain access to that SD card and had access to the encryption keys, they could decrypt the results, change the results, modify the ballot images on that SD card to conform with those changed results, re-encrypt it, re-SHA/hash it, and resubmit that to the EMS and the EMS wouldn't know the difference. That's one scenario.

Second scenario, if you're actually transmitting data via network interface, they could do the same thing in what's known as a man-in-the-middle attack leveraging the 509 keys and those encryption keys in combination.

Q To do effectively the same thing that you just described with the cards?

A Correct.

Q In light of their importance to system security, how should encryption keys be stored or managed on the system?

A They should certainly be protected like the family jewels. You know, they are a critical component of the integrity and the surety of that election and the functioning of that system.

Q And is that topic covered in FIPS 140-2?

A It is. It's key management principles.

Q And in a nutshell can you describe for the court what FIPS 140-2 requires with respect to the storage and management of encryption keys?

A If they're contained outside of the actual encryption module themselves, then they must also be protected and encrypted.

Q All right. With respect to Appling, Bibb, Coffee, Jones and Telfair, can you describe what you examined?

A Yes. So I was directed to a website, zebraduck.org, I believe is the name of that --

Z-E-B-R-A-D-U-C-K.

Q Will I need a witness to explain that name?

A I will have to rely on other outside experts to explain the name.

I was directed to this website, and it contained the responses from public records requests throughout the state of Georgia. Those four counties were part of those postings on that website.

They were posted there in the form of a zip file, a seven zip file, so it has a .7Z extension on it. I downloaded those files and extracted them. The first thing I did was I looked for a verification hash for the databases. When I did not initially see that on the first download, I queried back to the organization that posted them, and they provided us another link to a site that they had the original files that were placed up there, and those did have the seven zip file of the whole package and of the accompanying SHA value for those files; so I downloaded those, as well.

Q All right. And did you do anything to determine if the files you examined were authentic?

A Yes, I did.

Q Did that vary by county?

A The procedure was the same. Obviously, the files that I checked were different. You know, one has a name "X" and this one has a name "Y." However, the first thing that I did was I created my own SHA value for the seven zip file that was related to each county. I then compared that SHA value to the SHA value that was posted by the Dominion system in conjunction with the production of this package.

Q And what did you find?

A So on three of the counties they matched perfectly. In one of the counties, which was Jones, there was a mismatch, and so I further examined that particular mismatch and determined that at some point someone had mistakenly added that SHA value to the seven zip package for the encryption and that had changed the value.

I further dug into that particular package specific to the database file and the project package, that XML file, and determined that the dates and times of that file matched what was produced with the Dominion voting software.

Q Based on your examination, as you have just described it with respect to the backup databases in the four counties, do you have an opinion, professional opinion, as an expert as to whether the

files you examined are authentic?

A Yes, they are.

Q All right. Now, you -- are you familiar with how the Dominion system works?

A Basically, yes.

Q And how are you familiar with it to that extent?

A I've been examining these systems since 2021. I've actually created virtual machines of the forensics imaging that we have taken, and I have operated the systems in a virtual isolated environment.

Q All right, sir. Now, can you characterize the fidelity of the backups to the operational databases on the machines?

A Well, I can tell you that I had the unique opportunity to have a forensics image of Coffee County with that database in its operational state, and so I did examine the Coffee County database. I compared the artifacts of that database to the backup databases we received, and they are fundamentally the same construct and they would represent the operational databases of those counties.

Q And does that provide a reliable factual basis for the opinions you have given based on your

analysis of those databases and the encryption keys that are in them?

A Absolutely. If it exists in that backup database, at that point in time when they made that backup all of those -- all the data in that backup existed in the operational database.

Q Now, you've mentioned Coffee County a couple of times, and you've made reference to a forensic image. Would you please describe to the court how you came into the possession of the forensic image?

A So by direction of my attorney I was given access to a download site from a firm called Sullivan Strickler, and Sullivan Strickler had been engaged by Coffee County, or some person, to perform a forensics preservation of the Coffee County EMS, ICC, the Dominion-supplied laptop and some poll pads.

Q Okay. And how -- when you went on there and retrieved it, what did you retrieve?

A So when I downloaded those files from the secure website, the first thing I did was verify the images. And in this particular case, all of these images were in an EnCase image format, which I know well. It's a forensically preserved, a bit-for-bit copy of that device that was the target of that imaging operation.

It is a self-verification mechanism, as well, so when you verify a forensics image in EnCase it will tell you if any bit of that data is changed or if it's deviated from the original hash value at the time of the imaging of that device.

Q And what did that software report to you about the Coffee County image that you examined?

A They verified.

Q And in your field of work, cyber forensics, is the EnCase image, through the method you've described, considered to be self-authenticating?

A Yes. Not only self-authenticating, but it's the industry standard for admission into court.

Q So in your expert opinion both the Coffee County files you examined and the files from the other four counties are, in fact, authentic digital records of the systems in those counties?

A Yes.

MR. MacDOUGALD: At this point, Your Honor, I would renew my tender on the four counties, the flash drives. I don't have a flash drive or EnCase image or anything like that for Coffee, but I would intend to ask him questions about Coffee, you know, subject to the ruling of the court.

THE COURT: I think I already conditionally admitted them, so if there isn't any update from Mr. Tyson, I think we proceed along those lines.

MR. TYSON: Your Honor, I think we're just waiting for a copy, but we don't have any objection to them.

MR. MacDOUGALD: All right. So if they're authenticated, then we can dispense with my authentication witnesses. Several of them are outside. So -- and we can release them from sequestration.

THE COURT: All right.

MR. MacDOUGALD: You can let them know they can come on in.

Thank you, Your Honor.

BY MR. MacDOUGALD:

Q   What, if anything, did you do to check on the encryption keys in the election databases that you looked at in these five counties?

A   So the first thing I did was to verify their existence. I knew which tables they would reside in. I navigated to that location of those tables and verified that those encryption keys were there, and I did that in each of the five counties.

Q And is it your opinion that the encryption keys that you found in the backup databases in the four counties are the same -- in the same state or condition in terms of storage as they are in the operational databases for those counties?

A Yes. The reason that you make a backup is so you can immediately restore that backup copy to an operational state in the event that something goes bad with the EMS server during an election. So, by definition, those encryption keys would have had to have been the same as the encryption keys state in the operational database.

Q All right, sir. And so when you looked at these five databases, what did you find in terms of how the encryption keys were stored?

A In all five databases those encryption keys were stored in unencrypted text, open text.

Q Was there any control on access to the encryption keys?

A Not really. And the reason I say "not really" is because in the Coffee County EMS and in all other Dominion systems which I have examined, they're utilizing a user authentication to the database. So that means that if you are at the keyboard of the computer, then you have access -- full access to that database.

So the vulnerabilities for a Windows system are well known, the antivirus had not been updated since the Coffee County Dominion Suite had been installed in September of 2019. There's roughly 1 million new exploits released every day, and so when you do the math you're talking about millions of additional vulnerabilities that that system would not have detected. There were no system patches applied.

Once again, hundreds of vulnerabilities that were admitted by the operating system owner, Microsoft. They release a patch every Thursday, so the fact that that hadn't been updated after the installation of that Dominion software, you know, is -- it's just basically an open state. You know, we've heard other experts say that it's just wide open, and it really is wide open.

Q Does what you have described with respect to the storage and management of encryption keys on the election system in Georgia comply with FIPS 140-2 as a technical matter?

A No.

Q Is that a close call?

A No.

Q You may not know the answer, but does it comply with the Voluntary Voting System Guidelines as a technical matter?

MR. TYSON: I will just object on the lack of foundation. I don't think we've talked about the VVSG --

MR. MacDOUGALD: Well, you're right. I'll take it back, if I can.

BY MR. MacDOUGALD:

Q Are you familiar with the Voluntary Voting System Guidelines provisions on cybersecurity?

A I've reviewed them, yes.

Q Do you know enough about that to say whether the management and storage of the encryption keys on the election systems in Georgia complies with the Voluntary Voting System Guidelines?

A They do not.

Q All right, sir. Have you examined any Dominion election systems in other jurisdictions outside of the state of Georgia?

A I have.

Q What jurisdictions?

A Arizona, Pennsylvania, Michigan, Colorado.

Q And on those systems did you check on how

the encryption keys were stored?

A I did.

Q And what did you find?

A I found they're stored in the same state, which is plain text.

Q Unencrypted?

A Unencrypted.

And I might add that with those different analyses, it's not only that they're in the same storage state but Georgia uses Democracy Suite 5.5 Alpha, Arizona used Democracy Suite 5.5 Bravo, and Colorado used Democracy Suite 5.10.

Q And so those are subsequent updates of the system?

A That's correct.

Q But they all had the same characteristic?

A Yes.

Q As a matter of cybersecurity, how would you characterize that situation?

A Well, it depends on how I'm looking at it. If I'm looking at it from a hacker's point of view -- hallelujah. If I'm looking at it from a cybersecurity perspective, I can't believe that anybody would ever do this. You know, you're talking about the criticality of the -- ensuring the integrity of the vote, which is the base for our democracy, then how could you ever leave this unprotected? So I find it, frankly, appalling.

Q If a representative of the Secretary of State made the statement that Georgia's election system was the most secure in the world, what would be your opinion about that statement?

MR. TYSON: Your Honor, I'll just object here in terms of it's about the election system, he's not an expert on that. I don't think there's any basis or foundation for him to have known every election system in the world to respond.

MR. MacDOUGALD: Okay. I'll withdraw the question.

BY MR. MacDOUGALD:

Q Mr. Cotton, would you describe the Dominion system that you've examined in the five Georgia counties and in other jurisdictions around the country as the most secure computer election system in the world?

A I would not.

Q Second place?

A No.

Q All right. You had an opportunity sitting

in the courtroom to observe the demonstration videos that Mr. Parikh played for the court.

Do you recall that?

A I do.

Q And can you give an opinion about the significance for cybersecurity purposes of what those demos show -- and you can do them one at a time or you can do them in the aggregate.

A So basically what it shows and demonstrates -- and by the way I have performed independently each and every one of those activities to ensure that they are accurate. So what I can tell you is that those are just three snippets of vulnerabilities and methodologies by which you can gain access and manipulate this system.

But it does show a general lack of security within the voting systems, specifically within the database, and that database is critical to recording and reporting the results of an election.

I also have the advantage in this particular case to have access to the full forensic image of the Coffee County EMS, and so I took that one step further. I said, well, are those passwords present as the Windows user authentication passwords on any of these systems from Coffee County. And so I analyzed all of the passwords for the user accounts for the ICC, the Dominion-supplied laptop, and the EMS, and the dvscorp08! was present as the primary password for all of the accounts on the Coffee County adjudication system.

So now you not only have a vendor-supplied password in the SQL database, but you've got a vendor-supplied password for the only mediocre protection of the database. So basically what is demonstrated here is a total lack of cybersecurity with respect to the Dominion EMS and the voting system.

Q All right. So that was the password video, if I recall correctly?

A That is correct.

Q It showed us dvscorp08!

The second one -- do you recall what the second one was about?

A The second one was the tabulator passwords, and those were encrypted passwords that are contained within the election definition file and also the election database.

Q And the encryption keys were used to decrypt those passwords?

A Yes.

Q Is that method of password management compliant with cybersecurity standards as you understand it?

A No.

Q What is the significance from a cybersecurity password of having common user names and passwords for all the users?

A Well, there's a couple of very critical key points here. One, you're using a -- the same user name for every single account on the tabulators. As well as on the Coffee County EMS, there is a standard list of generic user names that are present on every single Dominion voting system that I have examined. Okay?

If the passwords are all the same and the user names are all the same, then there is no accountability as to who did what in the event that you do find something wrong. So you don't know who did it. Right? Furthermore, over time, if someone -- like in the case of an election worker, is a volunteer in one election, they would have that same user name configuration piece specifically for the databases for the next ten years or until they change them.

So, you know, the -- that really broadens the extent to which someone can exploit these vulnerabilities, and there's no accountability for those.

Q All right, sir. So if I understand you correctly, the user name and password in Colorado was the same as it is in Bibb County, Georgia?

A For the specific user names in the SQL database, yes. Okay. For those three specific user names it's dvscorp08!. What I have found is that specific to the Windows login you have the same list of user names and then a shared password for all the different accesses to that Windows system.

So what this means is that if you have a -- if you're trying to regulate what privileges a specific user has -- say, you want them here at the EMS user level, they can use the very same password to simply jump up to the EMS admin and have full control over that system.

Q And so we heard testimony from Mr. Parikh that the dvscorp08! password has been present on the system identified as a vulnerability since no later than 2010?

A I would submit that given the nature and the syntax of the password, probably since 2008.

Q How would you characterize that as a cybersecurity matter?

A Horrendous.

Q In your examination of any of these Dominion systems have you seen any indication of non-election personnel remotely accessing a Dominion system?

A Yes.

Q Can you tell us about that?

A I, too, have reviewed a series of e-mails produced by Dominion in which they're discussing remoting into Gwinnett County, Georgia. I have also reviewed depositions from Coffee County in which the election clerk specifically details how two Dominion employees fixed her voting system from the parking lot.

MR. TYSON: Your Honor, I'll just object here. I think we're into triple hearsay at this point at least.

THE COURT: Unless you've got an exception that comes to mind, Mr. MacDougald, I think I agree with that.

MR. MacDOUGALD: I don't think I can think of an exception, Your Honor.

THE COURT: All right. It will be sustained.

Next question.

BY MR. MacDOUGALD:

Q All right, sir. Have you at any point had any discussions with anyone from the Secretary of State's office about the encryption keys issue?

A I have.

Q Can you tell the court about that, please?

A In the Supreme Court affidavit I had mentioned that I had analyzed a Bibb County database, and we immediately got a call from the Secretary of State's office and correspondence demanding to know how I got access to the Bibb County election system.

My attorney that represented me at that, Mr. Kurt Olsen, handled those communications, primarily, but we did have a Zoom conference. I can't off the top of my head recall every person that was there as part of that conference, but they're all representatives of the Secretary of State's office.

Q And what was the topic of discussion in that call?

A They had misread the declaration and they had thought that I had access to the physical voting systems -- that I had analyzed the physical voting systems, not just the database.

Q All right. And was there any discussion of the encryption keys or your findings and opinions

on that topic?

A With the call, no; however, the very fact that the only reason they were calling me was because I had called out the encryption keys in that declaration they would have had knowledge of the issue.

Q Did they ask you any questions about the encryption keys' vulnerability?

A No.

Q Was there any discussion about what ought to be done to mitigate that risk?

A No.

Q And when was that?

A That would have been in the July time frame, I believe.

Q All right.

THE COURT: Can you put a year on that?

THE WITNESS: '24, Your Honor.

BY MR. MacDOUGALD:

Q Okay. I am going to ask you --

A I take that back. It would have been two days after the submission of the -- of that document in support of the Supreme Court petition.

Q All right. And I'm going to ask you to turn to Tab Number 5.

A (Complies.)

Yes.

Q And that's a document marked as Exhibit 5.

Have you ever seen that before?

A Yes, I have.

Q Now, this is an e-mail thread, and to be fair, you are not shown as being a sender or a receiver; is that correct?

A That's correct.

Q So how is it that you're familiar with the document?

A I was shown this by the attorney.

Q All right, sir. And does this refresh your recollection of when, approximately, your conversation with the Secretary of State's office occurred?

A Yes, this says Sunday, August 25th.

Q Well, let's go back down a little bit.

A Yeah, the thread looks like it originates March 28th.

Q All right. And it's fair to say -- or did the Secretary of State's Office ever follow up with you to talk about what your findings were?

A No. No. Once we had sent them the data on where we had obtained the backup file, that was the last I heard from the Secretary of State.

Q Is compliance with FIPS 140-2 an ongoing obligation as you understand it?

A Absolutely.

MR. TYSON: I'll just object on the grounds of obligation to what and under what?

MR. MacDOUGALD: I'll rephrase the question, Your Honor.

BY MR. MacDOUGALD:

Q As a technical matter, cybersecurity technical matter, is compliance with FIPS 140-2, where it's applicable, an ongoing requirement that must be maintained?

A Yes, absolutely. I mean, it would be absolutely ludicrous to require something for certification and then say that as soon as you buy the system you can do whatever you want with it -- you can delete the encryption keys, you can do whatever you want with it. It's nonsensical.

MR. MacDOUGALD: Your Honor, I'm trying to skip things that have already been covered with Mr. Parikh, so give me just a second. I'm almost done.

BY MR. MacDOUGALD:

Q You heard Mr. Parikh's testimony on how

X.509 certificates are used?

A That's correct.

Q Any disagreement with the way he expressed it?

A I would actually expand on it just a little bit.

Q Okay.

A So the opportunity I've had to look at different systems across different states gives me a unique perspective of what that vulnerability could do, and so that 509 value is the same in every single Dominion system that I've looked at regardless of version and regardless of jurisdiction.

What that means is that if anyone with that certificate can get access to the same network address space, then they can remotely establish trust with that voting system, execute APIs or direct interaction with that system without really needing to know the user password for the Windows system.

So I used the term "address space" because each of the Dominion EMS systems comes with pre-configured tunneling protocols and capabilities.

Q What are those?

A So a tunneling capability -- think of it as a VPN. If you've ever used a VPN to login to your office or somewhere else, you simply connect to a VPN and you have the same IP address or the same IP address space as the network that you VPNed into.

So in the case of the typical home network, that would be a 192.168.1.X network or address space. And so you could join that network and be a member of that network through those tunneling protocols. That is very easy to do. We do know in many jurisdictions that the routers that are procured as part of the Dominion Voting Systems are what they call managed switches which means that you can program access control lists, you can program routes, and you can establish tunnels to those routers. So, you know, that is -- it's critical that with that 509 key -- literally, if they have a tunnel, anyone, anywhere in the world that has access to that address space could change the voting software, they could change the voting results, they could change any aspect of that voting system that they desired.

Q If they did that, would it be detectable?

A Not given the current logging levels and the artifacts that they currently log. So the only way that you would detect that would be to analyze different machine address -- they call them MAC addresses. And those addresses can be spoofed, but generally they're not. But if you had a P-cap capture, which is a -- basically as you transmit data over a network those are in packets, and a P-cap is a packet capture.

If you have recorded those packets as they transmitted the network, then you may be able to determine whether or not somebody had unauthorized remote access. But given the current state of every system that I've looked at, they simply do not record P-cap data, nor do they record the system process data that tells you exactly which processes were executed on the system. So the short answer is: At the current state, no, that would not be discoverable.

Q Can Dominion remotely access these systems without detection?

A Based on the e-mails that I reviewed, yes.

MR. TYSON: I'll object just on that basis that -- because we're relying on hearsay for that.

THE COURT: If you want to expand on the basis for his opinion.

BY MR. MacDOUGALD:

Q What's the basis for your statement.

A Dominion produced a number of e-mails in response to subpoenas. A number of those e-mails have been released publicly by a sheriff by the name of Dar Leaf, and contained within those e-mails are specific conversations about them remotely accessing voting systems during the course of an election.

Q Apart from that, based on your understanding of the technical aspects of the systems, is that possible to remotely --

A It is possible.

Q Okay. We've heard reference to air gapping. How would you characterize the level of protection provided to the Georgia systems by the Georgia version of air gapping?

A Well, air gap is a technique, but it's an easily bypassed technique for protection. The U.S. government has been bypassing air gap networks since the '70s, okay. And the most common technique to bypass that is called island hopping. And basically we know that the EMS servers typically have a wireless card installed on the motherboard, even though they claim it's disabled, it's still there.

If you bring in a hockey puck with an unencrypted signal, typically default on a wifi is to connect to these unprotected wifis, so all it would take was somebody with their cell phone in a hot spot mode or bring in a Verizon hockey puck, and once that

EMS connects to it or any of the other systems connect to that, you bypass the air gap network. It's very rudimentary.

If you've got an actual active insider threat, it's child's play. If you have somebody who is inept in configuring systems -- it happens all the time, so it's -- it is a technique for protecting, but it can't be the technique, because it's so easily bypassed.

Q All right, sir. And -- so if we assume that this system is vulnerable because of the encryption keys and the passwords as we -- and the X.509 certificates, as we've discussed, are the physical security measures that are supplemental to electronic cybersecurity, are they sufficient to protect the system?

MR. TYSON: I'll object, Your Honor, on the grounds that I don't think that there's foundation for Mr. Cotton's knowledge of the physical security measures that Mr. MacDougald's question is referencing.

BY MR. MacDOUGALD:

Q As a general matter as a cybersecurity professional, can you rely on physical security procedures in place of adequate protection of

encryption keys and passwords?

MR. TYSON: Same objection. I believe we're talking about a specific set of physical security processes in Georgia that we haven't established he has knowledge of.

THE COURT: All right. So, yeah, Mr. MacDougald, can we tie it a little more closely to Georgia practices and procedures? I also say -- I think we've already covered this ground fairly adequately, and so I really don't know what additional insight he might offer here.

BY MR. MacDOUGALD:

Q Okay. So as a general matter, are you familiar with the concept of physical security in the cybersecurity world?

A Yes. And in the course of my support to election litigation I have visited various election offices, shall we speak, although I have not visited Coffee County, but it's important to remember that the people who run our elections are not cybersecurity experts like myself and Clay. In most cases these EMS servers that I've viewed are simply running in the clerk's office. So while you may call it an air gap system, there's a question as to physical access on these systems if they're simply exposed in a clerk's office and they're there 24/7.

Q As a cybersecurity professional, would you be willing to rely on physical security measures as the primary defense of your system where it was as vulnerable as the Dominion system is, as we've discussed?

MR. TYSON: Your Honor, same objection in terms of Georgia specific -- we're assuming a lot without foundation.

MR. MacDOUGALD: I'm asking that as a general matter.

THE COURT: All right. I'll give you some leeway, Mr. MacDougald. We're getting a little astray from the core of your petition, but we'll see where it goes.

THE WITNESS: Certainly physical security would be an aspect of it, but I would heavily focus on what happens when that first layer of defense breaks down. Right? So if your defense on a system is strictly one layer, and that breaks down, then you really have no layers. We had a saying in the military that one is none, two is one. So in this particular case if you're solely relying on physical security to ensure the protection of those encryption keys, then that's really not security at all.

BY MR. MacDOUGALD:

Q Do you have familiarity with the physical security procedures in Georgia election processes?

A I have been informed by the clerk from Coffee County what her procedures were. I am not familiar with the total statewide standard operating procedures.

Q All right, sir. Now, in the -- there was testimony earlier that there are lots of different vulnerabilities for the election system. Can you assign a rank to the encryption keys and password vulnerabilities and X.509 vulnerabilities that we've been discussing relative to the other known vulnerabilities? Can you rank it?

A In some ways they are different classifications of vulnerability. So most of the vulnerabilities that we've talked about are really vulnerabilities to grant access to those systems that contain the unsecure keys. Okay? So the relationship between those two different categories is if you've got a vulnerability over here for access, then you've got the full vulnerability for the encryption keys in effect.

I would say that if you're going to rank this, I agree with Mr. Parikh's assessment that the average home computer is better protected from a cybersecurity perspective than the EMSs that I have examined. And I'll take this kind of one step further. 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 taut that security on that bank fault, 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.

Q And as an incident response professional, would mitigating that be a high priority?

A Absolutely.

Q What mitigation measures could be taken in the way of transparency that could help mitigate this that wouldn't be overly burdensome to the counties or the state?

MR. TYSON: Your Honor, I'll just object here. I think overly burdensome to counties and the state assumes a level of knowledge this witness has not -- there's been no foundation for that, and this is very speculative, even for an expert, on what he could offer.

THE COURT: All right. Sustained on those grounds. Rephrase.

BY MR. MacDOUGALD:

Q All right. Would it be difficult to order the election officials to produce system logs, cast vote records, and ballot images shortly after the election?

A No, it would not.

Q Would that affect the user experience at all?

A No, it would not. And furthermore I would say that if you're really going to protect and mitigate during the time frame while they're fixing the database encryption issues, you would also want to unable P-cap captures of the network space so that you could definitively prove that nobody else remotely accessed those systems, and enable what's known as SIS log logging of the actual processes and operating system to determine what programs and processes were ran during the course of that election, and both of those are very simple technologies and are not burdensome at all to implement.

MR. MacDOUGALD: All right. Thank you, sir.

THE COURT: Unless there's an immediate need for a quick break, I'd like to see if we can power through.

Mr. Tyson?

MR. TYSON: I don't expect to take as long with Mr. Cotton.

Good to see you, Mr. Cotton.

EXAMINATION

BY MR. TYSON:

Q   Let me start with Coffee County, because you've reviewed data from Coffee County, the forensic images you described, right?

A   Yes.

Q   And were you aware of data collection happening in Coffee County before it occurred?

A   No, I was not.

Q   Do you recall when you first were hired to review Coffee County's EMS and equipment?

A   That would have been the end of May first part of June of '21.

Q   And I believe you indicated you worked with Stefanie Lambert; is that right?

A That's correct.

Q And it was your understanding that Misty Hampton, the then elections director in Coffee County, was a client of Ms. Lambert's; is that right?

A Yes.

Q You referenced a firm called Sullivan Strickler that you used -- utilized to download those images.

Do you know who Sullivan Strickler's client was in the Coffee County election?

A I do not.

Q And you've been involved in imaging election equipment in states other than Georgia, right?

A Correct.

Q And that includes voting equipment in Michigan?

A Yes.

Q Was that also working with Ms. Lambert?

A Yes, and part of that was also Matt DePerno.

Q You indicated you conducted a forensic examination of the Coffee County images.

What do you mean by that term?

A So forensics means I applied standard

investigative practices that are technically accurate and repeatable. The term "forensics" means that you're gearing this towards admissibility into a legal environment and so it must be able to be replicated and must be authenticated.

Q In your review of the Coffee County images you didn't find any malware, did you?

A I did not find malware.

Q Did you find any evidence of any deletion of votes on those systems?

A To the extent that I have looked at it at this point, no.

Q And earlier when you referenced you had spoken with the clerk in Coffee County, were you referring to Ms. Hampton?

A Yes.

Q And so you've spoken with her about her work in the Coffee County elections office?

A Yes.

Q And you're aware that Ms. Hampton and others were criminally indicted related to allowing access to the Coffee County equipment, right?

A I read about that in the newspaper, yes.

Q I believe you said you've never been to Coffee County; is that right?

A No.

Q So let me ask you about some of the analysis you performed. You described some different ways that people could access systems, and one of the things you described was a similar pattern, I believe, of vulnerabilities in Dominion equipment in states other than Georgia; is that right?

A Yes.

Q And so a way to think about this, it's not unique to Georgia to have these encryption keys stored the way they are. To your knowledge, every state that uses Dominion equipment has the exact same vulnerability, right?

A Yes.

Q So when you said the Georgia system, in your view, is not safe and secure, you'd agree that that applied to other states using Dominion equipment, as well, right?

A I would.

Q In terms of access to a system, you described some ways where if somebody had access they could undertake various steps. Do you know, or have you reviewed in Georgia, any rules surrounding the storage and maintenance of voting equipment?

A I have not.

Q So you don't know exactly what someone would need to do to gain access to the Dominion equipment in Georgia, right?

A I mean, basic storage is basic storage. So if you have it secured, it's locked up somewhere in a closet, somebody has to control a key. However, Dominion systems have to be maintained. You can't let the batteries go down on the tabulators, you've got to keep them plugged in, you've got to keep them energized, so someone has to maintain them, so there is continual access during that time period in which they are stored.

To the extent of who has access, I do not know, but from a -- from a basic principle perspective, if you secure something people have access, they perform maintenance throughout the year.

Q You talked with Mr. MacDougald about air gapping. You'd agree though air gapping is a security technique of some sort, right?

A Yes.

Q And you discussed a scenario where someone could bring in a hockey puck to connect to wifi, various things like that. Has that ever occurred in a Georgia election to your knowledge?

A So here's what I will tell you is I have, in the course of my examination of Coffee County, that system was connected to the internet. Now whether that was through a hockey puck or another routing mechanism I simply haven't been able to determine what that is, but the artifacts on the system itself mean that it was connected to the internet.

Q And when you say "connected to the internet" are you finding artifacts of network connectivity or specifically internet connectivity?

A Internet connectivity. For example, I believe it's mail.live.com where somebody checked their mail.

Q And was that on the EMS server or on another component of the system?

A It was on the EMS server.

Q And do you know if that connection of the EMS server to the internet would be a violation of any Georgia law or regulation?

A I would assume that it would be given what I know about the Georgia law.

Q You talked with Mr. MacDougald about different risk mitigation strategies that are on the EAC website.

Do you recall that?

A I do.

Q And you'd agree that states may select different risk mitigation strategies based on things that are unique to those states, right?

A Yes, however at a certain point there has to be a little bit of common sense involved in that risk analysis. Right? So if you're saying that I'm going to assume a wide open barn door because I really like the looks of the lock when it's open, then obviously that's a failure of the analysis in the risk mitigation strategy.

Q Now, from your review you'd agree that the encryption keys for each of the databases that you reviewed while they're stored in plain text were different for each county, right?

A They were.

Q And as part of your analysis in this case you've never reviewed the process Georgia uses to build election project files, right?

A It's my understanding that's controlled by the state, and that in and of itself may be a weakness from a security standpoint because you have one office who is now constructing all of the project files, thus defining all of the passwords for every single county in Georgia. So there's a single point there where all of that information is in one point. So the fact that

that is performed at state level in one location is actually a weakness rather than a strength.

Q Do you agree that it's better than having a vendor perform that function of building ballots?

A I think that would depend probably who at the state is doing it. If you have the janitor doing it, then I wouldn't say that, but typically I would agree with the statement that if you have competent people at the state level performing these functions that are government employees, then that gives a larger fiduciary responsibility and assurance to the process.

Q And you haven't reviewed the process Georgia uses to deliver election project files from the state to the counties, right?

A No.

Q In response to questions from Mr. MacDougald you proposed some other changes you think need to be made to the Dominion system, P-cap captures, I believe -- various things like that.

Do you have any knowledge of whether making changes like that to the Dominion system would alter its current EAC-certified status?

A Well, the beauty of those changes would be -- like for a P-cap capture, that would not involve the Dominion systems at all. That would simply be what's termed a tap off of the switch in a promiscuous mode so that it would record all of that traffic. So there would be no impact to the certification status of Dominion at that particular point.

The syslog enabling function is a setting in the registry. It would require a repository to be established external from the voting systems themselves, because you don't want to put the copies of the logs on the same place where you caught the logs from. That should not affect the certification status.

But I find that argument a little bit interesting because on one hand you're saying you can't do a simple configuration change because it may affect the certification, but on the other hand in my certification -- or in my analysis of the Coffee County voting system, there is a compiler on that system and they have developed, modified or created over 3,000 program executable files or device drivers on that system and that did not affect the certification, apparently, of that system.

So in my view of that, it's -- you can't have your cake and eat it too. Right? You either allow changes within certain constraints or you don't, and in this case changing a registry setting, making a configuration to take the logs off of those individual systems and centrally store those for future analysis is minor compared to creating program files, creating DLL files, which can actually change and modify the behavior of the system.

Q So it's your belief that having those compilers is an additional vulnerability, but it's not something related to EAC certification; is that right?

A So EAC certification requires a static program listing as it relates to the voting system, okay. I'm going to leave legal opinions to the attorneys in this room, but what I will tell you is it's, once again, nonsensical to certify a system -- and actually the Secretary of State's Office called for, essentially, an audit after the 2020 election in which they hired Pro V&V to come in and certify that nothing changed on those systems, and at the same time have program files and DLL files that were modified and created related to Dominion Democracy Vote software paths, over 3,000 of them.

So, you know, in my opinion, if you change or if you add a program file or a device driver that's related to the voting software, that should decertify the system.

Q So to make sure I'm clear on my question then, you believe that the existence of compilers should result in a loss of EAC certification, but to your knowledge the Dominion 5.5A system remains EAC certified; is that right?

A So my opinion is that if you use those compilers to create new executable files or to create new or modify the device drivers of those program files, that should relate in a -- result in a decertification of the system.

Now, the problem is nobody checks. Okay? I know that when Pro V&V came into Georgia they said no file had been changed, but they didn't check the entire directory paths of the Dominion Voting System.

Q You gave an example of a bank vault and writing the combination and putting it on the door of the vault.

Do you recall that?

A I do.

Q You'd agree that even if a bank undertook that, having locked doors on the outside of the building and having guards or staff present would at least provide an additional layer of security, right?

A Well, it would provide an additional layer. Now how effective that is is, you know, obviously the question. And, you know, if this -- if I can relate to an old show, and I'm dating myself here, if you've got somebody guarding it whose name is Barney Fife, and he's got one bullet, and he's asleep in the car, then that's really not protection, but it is a technique.

Q And you've obviously looked at some components of the Georgia election system. Do you have any evidence that anyone has ever manipulated votes in a Georgia election using any of the vulnerabilities that you've described in your testimony?

A The challenge is that you're not recording the right items or enough of the ones that you do record to make that determination.

Q So that would be a you do not have evidence, correct?

A Well, just as I would argue that you can't definitely prove that they didn't. There simply is no proof there because you don't have the necessary elements to analyze to determine whether or not, prove or disprove, that something happened.

Q So for whatever reason you don't have whatever tools you feel you need to have, it's still true that you don't have any evidence of manipulation

of votes cast in a Georgia election, right?

A Based on the forensics evidence, if you have no evidence -- or no artifacts to look at, then you're right.

Q Mr. Cotton, do you believe that Georgians can never know for sure whether Joe Biden won the 2020 election in Georgia?

A Look, I served my country for 21 years --

Q And we appreciate that. Thank you.

A -- and I abide by the law of the land, and he is our certified president. Okay. This is not about rehashing the 2020 election. This is about restoring the confidence and faith of all Americans in the foundation of our democracy, which is the voting process. And if we can't prove or demonstrate to them that this process is secure and that we can detect if there is something going on, then I think that what we saw subsequent to the 2020 election is going to continue forward into the next foreseeable future with whoever lost bringing these up as issues before the general public.

And so I really look at this as more of a confidence issue and making sure that we, as a collective government, are doing the steps that we need to do to ensure the integrity of these elections.

Q Is it your testimony that if no changes are made to the Dominion system as it's currently configured that Georgia voters cannot trust the results of the 2024 election that will be happening in November here?

A I'll go you one further. I mean, you know, there's obviously going to be doubt. If no steps are taken to address the vulnerabilities and the integrity issues that are readily knowledgeable in the public, then there's going to be doubt. Okay? But I will go you one step further. In those e-mails that I have reviewed the Dominion programmers themselves stated --

MR. TYSON: And I'll just object here to hearsay, Your Honor, to any further testimony on that.

If I could have a moment, Your Honor? That's all the questions I have, Mr. Cotton. Thank you.

THE COURT: Any redirect on those points?

MR. MacDOUGALD: Just a couple, Your Honor.

FURTHER EXAMINATION

BY MR. MacDOUGALD:

Q You mentioned the executable files?

A Yes.

Q Were those placed on the system or were you able to tell whether those were placed on the system before or after certification?

A They were placed on the system after EAC certification and after the installation and implementation of the Dominion software on the Coffee County EMS.

Q And does that raise any questions in your mind about whether the certification is still valid for that particular system?

A Huge questions. Huge questions.

Q Now you mentioned a compiler. What does a compiler do?

A So, you know, as experts we are often accused of speaking very technically and --

Q Yes.

A -- above people's knowledge levels, right?

Q And you are guilty as charged.

A I am guilty. So a compiler does the same thing for a computer. Okay. So a computer only understands one language, zeros and ones, bits and bites. Okay. Now as humans we like to program in programming languages, okay, and they can be C++, it can be COBOL, it can be Fortran, it can be, you know, Net++, you know, tick, tick, tick, tick, tick. What a compiler does is takes that human written code and turns it into machine executable language so that the machine knows how to interpret it and run appropriately.

Q Is that compiler a necessary component of the ordinary functioning of the election system?

A Well, here's what I would say. If the Dominion software requires changes to a program for an election cycle or requires the development of a new device driver, then that clearly would be outside of what the scope of the certification examination was in the EAC.

Now, whether it's required or not, that would be an EAC and a Dominion question. Okay? Why do we have over 3,000 program files and device dynamic link libraries, which are device drivers, that were created or modified after you installed the software, and they all appear to emanate from the Net++ MSBuild.exe compiler.

Q Which was also installed after the original installation?

A No, that was installed before. So what's changed -- so it appears that the Net++ MSBuild.exe was installed as part -- or that it was part of the golden image that was utilized to install the Dominion software when it was -- when it was created, when they created the EMS. But what's different is that it was actually used, and it actually created over 3,000 executable files and .dll after the fact.

Q   That were not part of the system at certification?

A   Correct.

Q   Can the compiler be used by a bad actor?

A   If you have access to the machine you have access to the compiler.

Q   And what possibilities does that open up?

A   Well, you know, I spoke a little bit about the OPM breach. In that particular case the piece of malware was actually a dynamic link library file, a DLL file, that was masquerading as a McAfee antivirus driver, and that created the entire access to the system, the exfiltration path, it created the entire vulnerability for that system.

So when you're talking about malware you're talking about unauthorized access, unauthorized exfiltration, and those types of things, the creation of specific DLL files or executable files is quite common, which is why they should not be there after the certification.

MR. MacDOUGALD: All right, sir. That's all I have. Thank you.

THE COURT: Any re-cross?

MR. TYSON: Just one question, Your Honor.

FURTHER EXAMINATION

BY MR. TYSON:

Q Mr. Cotton, just so -- I think we're all clear on this point, but is it your understanding that Dominion 5.5A is certified by the Election Assistance Commission right?

A I have seen the certification certificate.

Q Okay. So it is?

A Yes.

Q Thank you, your Honor.

THE COURT: All right. Can this witness be excused, Mr. MacDougald?

MR. MacDOUGALD: Yes, he may, Your Honor.

THE COURT: Thank you. You may step down.

Any further witnesses or evidence, Mr. MacDougald?

MR. MacDOUGALD: Subject to delivering the flash drives on the demos, no, and with that I think we've tendered everything that we've identified and intended to put in, and I think they've been ruled on, so we would rest at this point, Your Honor.

THE COURT: All right. So finding that the applicant's case in chief is closed for now at this point what I would say, Mr. Tyson -- how soon do you think you can get a copy of those flash drives to him either remotely or physically?

MR. MacDOUGALD: Well, this evening, electronically, tomorrow physically.

THE COURT: Okay. Do you have a preference? Do you need them both or is remotely fine for you?

MR. TYSON: Remotely is fine.

THE COURT: All right. If there's anything you need just let us know in the next day or so, Mr. Tyson, if you've got them, if you have any further concerns with those exhibits.

And then should, Mr. Tyson, you -- I think we're going to call that a day for now, and should we reconvene -- did the Secretary anticipate presenting any evidence of their own or any witnesses?

MS. YOUNG: Possibly, but before we do that we'd like to both renew our motion to dismiss and also make a motion for directed verdict.

THE COURT: Right, and I'll get to that in just a second.

I just kind of want to scope it out, and if you'll say just generally, kind of, what that would look like, if you have a proffer, generally, of what that testimony would be and just to kind of complete the road map for today.

MR. TYSON: So, Your Honor, I think if we end up putting on evidence it would be probably a single witness from the Secretary's office just to speak about some of the internal processes for -- I know we've had some different answers in terms of ballot building, delivery of the information to counties, those types of things. I believe the SEB rules can be decided as law. I don't think I need testimony on those. So I think that would be the substance of what we would be looking for in a witness from the Secretary's office -- so not very long.

THE COURT: Sure. Is there anything as it relates to encryption keys or their current status that would come in through that witness?

MR. TYSON: I don't believe so, Your Honor.

THE COURT: All right. Ms. Young, based on what you have heard in the case in chief, is there anything that you think needs updating in your arguments or that you want to highlight from what you learned today?

MS. YOUNG: Well, in terms of a directed verdict I'd kind of like to address why the evidence that you just heard is not sufficient to state a claim for mandamus, and I can do that this afternoon or --

THE COURT: I think we've got a little time here, so --

MS. YOUNG: Sure.

THE COURT: I guess, mainly what I was saying is obviously I'll incorporate all your arguments from the motion -- for the motion to dismiss. I'm more just curious what value you would have in addition to that. That's moreso what I was trying to press on.

MS. YOUNG: So a couple of things to say, if I can take the podium.

You know, I want to start from a big picture standpoint because, you know, we've heard a lot of testimony about the flaws that the petitioner's experts believe are in the system. And even if you take all of those as true, and even if you don't hear testimony that we might put on about the guardrails that are put around the system that keep some of the parade of horribles ideas from happening. They look at 300, and they say, well, that can't mean what it seems -- what they think it says. It can't simply be, you know, go buy a system that's certified and certify the system and you don't have to do anything else ever again, and they're kind of right and they're kind of wrong. That is what it says. But it doesn't say that in a vacuum.

And if you look at -- there's a great law review article at 36 Georgia State University Law Review, Page 86 -- I'm sorry, 81, and it kind of goes through the history of HP316 of which 21-2-300 was a part. And, you know, the use of the BMDs at that time were very hotly debated, and while we didn't hear this exact argument about encryption keys, there were arguments made against the use of the system.

And the law review article, kind of, goes through, kind of, the objections to that, and what came out of that was, okay, you know, the majority wanted to have a BMD system, but they said we're going to do certain things, buy a system that's certified, and then after that purchase you're going to have risk limiting audits and logic and accuracy testing. So when you look at 300, it's a starter statute. You know, it tells the Secretary, go buy a system that's certified. Then you look at it and you certify it yourself. And then from there other statutes kick in in terms of who is going to do what.

You've got -- and, you know, if you go through the entire election code, lots and lots of statutes that talk about what happens after that. You have statutes that tell the county superintendents that they need to make storage plans and they need to appoint a person that's going to be in charge of making sure the storage is safe. You've got this whole very detailed description of the counties doing logic and accuracy testing before elections and then a process for risk limiting audits after the elections.

From that point forward most of the responsibilities are placed on the county. The

SEB is told to go, you know, promulgate rules for recounts and they narrowed the threshold for the recount by a half of a percent to make it a little easier for somebody to meet that recount threshold. And so when you look at HB316 and our election code as a whole it makes sense that the Secretary's obligations under 21-2-300 did stop at that point, because that's when other things kicked in.

In terms of what we've heard today for a lot of things criticizing, you know, whether or not the system should have been certified or should still be certified -- the reality is, it's certified. It's still certified. And under 21-2-300 what the Secretary was to do was to purchase a certified system, which he did, and then certify the safety of that system, which he did.

What should happen today could be a matter of debate. Should the EAC change its rules? Should they do something? Those are interesting points to debate, but that's not a proper case for mandamus. You also heard -- is it Mr. Cotton or Dr. Cotton? I can't remember -- you know, admit that the EAC certification is static. That was a very clear admission that, you know, he acknowledged that that certification is static. Now, they have raised, you know, lots of arguments about why maybe it shouldn't be or, you know -- whatever, but the EAC isn't here, they're not a party to the case.

We've also heard about physical security not being enough. Well, the legislature thought that it was, and the people responsible for ensuring that, you know, some of these things that we heard about about election workers not properly watching their spaces -- those election superintendents aren't here either, and those are their duties under the code.

So when you look at mandamus, nothing that we have heard here today points to a clear legal duty placed on the Secretary that has been breached.

In terms of laches, you know, you heard testimony that people have been aware of this issue for quite some time, depending on which witness you're talking to, but, you know, even the plaintiffs --

THE COURT: Isn't it really only, like, one witness that matters, and that would be

Ms. McCarthy.

MS. YOUNG: True, but -- and she testified, you know, that she is a cybersecurity expert and that she read the Halderman report when it came out. And the standard for, you know, what puts you on notice of bringing a claim isn't, you know, having an ah-ha moment, it's having some knowledge that there's an issue and picking up your duty to investigate further.

If you look at the cases that talk about factors of laches, the ones that apply here are, well, you start with how long is the delay, and then you look at what's the excuse for the delay, and, you know, you heard these experts say they began working on declarations months ago without having a plaintiff, apparently. Apparently it was just a matter of time until they found one.

But, you know, between there not being a really good excuse for that delay, and then the final factor being, what's the prejudice? The prejudice is, well, we're starting early voting in about two weeks. This is not the time to be reevaluating the state's entire system. The legislature had a very clear plan with HB316, and they thought a lot about the steps in that plan. And the Secretary did the things the legislature told him to do. The county elections workers picked up the ball from there, and then from that point forward it was a group effort between the Secretary and the elections workers due to all of these things that the legislature sat down and, sort of, brainstormed out to try to help find a brand new system for our state and then take it from there to make sure it was securely stored, maintained, and properly checked before and after every election.

There's just simply no cause of actions here for mandamus, and so we think even with what you've heard today directed verdict would be appropriate.

THE COURT: All right. Thank you, Ms. Young.

Mr. MacDougald?

MR. MacDOUGALD: Thank you very much, Your Honor.

So the fundamental legal question, I think, presented by the motion to dismiss and the motion for directed verdict is whether there is a duty to -- of ongoing compliance with the certification requirements.

They say there isn't, we say there is. And we rely primarily on 21-2-300 sub-sections (a)(2) and (a)(3). And their argument relies on a very narrow reading of the language in (a)(3) that it shall be certified by the EAC prior to purchase, lease or acquisition, and we've checked that box, and that's all we have to do.

But that interpretation does not square with sub-section (a)(2), which requires that the Secretary certify it as safe and practicable for use. Now, that certification by the Secretary, it is made prior to purchase. That's a -- you know, that's relevant to the statutory analysis, but what is the purpose? What is the purpose of that certification? What is the purpose of the EAC certification? What is the purpose of the deliberations by the literature that Counsel has referred to about how to have a secure election? Well, the purpose is to have secure elections on secure systems -- voter verifiable.

Why do they store the machines in locked rooms? Why do they put sealing tape over the machines and the cases they're in? Why do they do all of those things? Why have any physical security procedures in an election? Why have any chain of custody procedures in elections? The entire structure of the election code in Georgia and the regulations that the Secretary -- the state election board has promulgated is to promote election integrity and give the public faith and confidence in the result and have an auditable trail so that people can trust the outcome.

So this is important, and Mr. Cotton talked about this. We're evolving into a situation of zero trust in the elections that was a big discord in our country over the 2016 election and whether it was hacked by the Russians. There was huge discord in our country over the 2020 election, and people are losing faith and confidence, and that creates a fragile situation, and we need a stable situation.

We need -- in a zero-trust environment we have to have verifiable steps and documentation and proof so that it doesn't require trust. It can be verified, independently -- it requires auditability.

THE COURT: So your interpretation of the statute, this certification, this isn't a one-time deal. That's your interpretation of this?

MR. MacDOUGALD: Right.

THE COURT: So this is a --

MR. MacDOUGALD: Ongoing requirement.

THE COURT: And how often? And something that could be revisited at any point? The Secretary could uncertify it at any point according to this statute?

MR. MacDOUGALD: Yes. There is a provision, and I can't recall the code section -- I'll get it to the court, I'll file a supplemental brief, that permits a petition to be filed with the Secretary. It's either competing vendors or a certain number of electors -- I think the number is 17 electors, and they can petition for the Secretary to revisit the question of certification. So that's a specific way to invoke a duty to reexamine the question.

But in this case we have the Halderman report which documents the encryption key vulnerability and many other vulnerabilities being delivered to the Secretary in July of '21.

It wasn't made public until June of '23. I think earlier I said July, and apparently that was wrong.

So what has the Secretary of State done in response to that? Nothing. In March of this year the Parikh -- excuse me, the Cotton affidavit in another case apparently came to the Secretary's attention and contact -- they reached out through the Secretary's general counsel to inquire about that. And that affidavit was made available to the Secretary's general counsel, and the gist of that affidavit is very close to the affidavit that was -- that we submitted from him as an attachment to our application and to the testimony you heard from Mr. Cotton and Mr. Parikh.

So the entire problem was laid before the Secretary in, I think, late March of this year. And what did the Secretary do? He did nothing. And so we are here asking for mandamus relief to compel the Secretary to do what he will not do himself. And the -- so interpretation of the statute we say it would be absurd to interpret it as the Secretary's counsel urges, because then it would be nothing more than security theater. It would create the illusion of security, not the reality of security, and we cannot impute to the legislature the intent to simply create illusions.

They wanted to create the reality of election security, as illustrated by the entire body of law in the election code regulating very, very minutely the procedures for carrying out elections.

The Secretary, his own self, took the position in the purchase contract with Dominion that the system must maintain compliance, so which is it? Are they supposed to maintain compliance as the contract provides or is it in the rear view mirror and it doesn't matter?

So the mandamus code sections 9-6-20 provides that -- in our brief I quoted this language, and I said it was 9-6-21. I was wrong. It's 9-6-20. It says that there's a -- mandamus provides a remedy for improper performance.

THE COURT: And I'm highlighting improper performance. The most common application we've seen is, do something, not that, you know, you've done it wrong. Do any particular cases stand out where the Supreme Court said you did it wrong, so do something.

MR. MacDOUGALD: Not on the remedy of compelling due performance, so that language in 9-6-20 would remedy for improper performance and compel due performance. So we think that it's a mandatory duty that the system comply with the EAC certifications, and that responsibility falls --

THE COURT: And I'm not just saying not just confined to the world of election law. Are there any mandamus cases that you came across where they said, yes, that performance was improper and here's the court stepping in to say that it wasn't proper? Or were they all just kind of mostly the complete absence of any action?

MR. MacDOUGALD: Well, the other statute, 9-6-21, it does say that there's a remedy for the -- normally it lies only for ministerial duties, but it's also black letter law that mandamus will lie for discretionary duties if there's been an abuse of discretion. And so if it's not construed as a mandatory duty, which we think it is because it either complies with certification or it doesn't, you know, and as we sit here today it does not.

And, you know, would the Secretary today in light of this evidence certify this system safe and practicable for use? I hope not. I attribute to the Secretary good intentions to have a secure system, but it's baffling that they have not reacted to the compelling evidence that's been in his hands for three years about this problem.

So mandamus, you know, that's the remedy. It's available to us, and we are resorting to it. So the abuse of discretion, if he -- let me put it this way: He doesn't have discretion to field a system that has open text encryption keys that any moderately-sophisticated attacker could exploit to alter election results without detection. He doesn't have that discretion. Where's the statute that says that?

And they get there -- that's the effect of the argument -- they get there by saying, well, all we've got to do is have a pre-purchase certification, then it doesn't matter anymore. It does matter. It has to matter. The only context in which it could matter is the operational context. The whole point is to have a safe election, not to pass a test.

And the -- why did the legislature require a test? So they would have a safe system in elections. It's nonsense to construe this as there being no duty -- no duty to have a compliant and safe operational election system. That's the thrust of the entire thing.

And so the -- I think -- I have not read that, Your Honor, but I will go out on a limb and say that an overwhelming concern was election integrity. The commission that was convened by the Secretary was called the SAFE Commission. It wasn't the unSAFE Commission, it was the SAFE Commission. Why? Because they wanted a safe system. And if those people had known that these encryption keys were in plain text, that you had hard-coded vendor passwords going back to 2008 or 2010, that you had 10-year X.509 certificates, that could establish trust between communicating machines, it wouldn't have gotten off the ground.

Now, we have an argument that's been made that -- I will paraphrase by saying there's so many different security problems on this system that it doesn't really matter that the encryption keys are in plain text. He did not say that, I'm characterizing it. But the line of cross-examination was, well, there are lots of problems here, and this is just one of them, and why should we focus on this one compared to the other ones? And the reason is because it is an extreme vulnerability and it's been proven in this courtroom they can be exploited to decrypt passwords with administrative privileges. It's been proven in this courtroom that they can be used to alter election results. Those are critical, critical, vulnerabilities, and they're not being addressed, and I am sad to say that the Secretary of State's office is resisting doing anything to correct them.

There was another sort of insinuation, you know, that it's the same all over the place. Well, that's like the "everybody does it" defense. You know, the question is, does it comply with the statute? Yes or no, and it doesn't matter what everybody else does. It either complies or it doesn't. And it does not comply, and there's no evidence that it complies.

Laches -- the actual test is gross laches. No illumination was provided on the subject of gross laches. The earliest that -- so Ms. McCarthy reads the Halderman report back in '23 -- that is June of '23. We're talking 14 months. Laches can be sometimes analyzed in comparison to applicable statutes of limitation. It's not in every context, but that is one way to sort of figure out where you are in the world of sleeping on your claims. There's no particular statute of limitations on this.

The public and the plaintiff were entitled to assume that the Secretary would perform his duty. And I cited this in the brief, it's the case about recording the lease. Oh, well, you knew in 2003 -- well, there was -- I was at pains to point out we got encryption key vulnerability as one part of it. The certification aspect of that problem is the other, and it's fair to say that Halderman talked about encryption keys vulnerability in July, '21. He did not talk about certification. He did not put it in the context of certification.

That report was such a hot potato it was put under seal. It went up to CISA, which is the Cybersecurity and Infrastructure Security Agency, and they've got security in there twice -- Cybersecurity and Infrastructure Security Agency. And they took about -- well, Mr. Tyson would know better than me, but I would say approximately a year to review that. They issued a bulletin recommending mitigating measures, you know, adaptations, you know, eight of them. They didn't mention encryption keys at all.

And the Secretary, from 2001, forward, has not taken any action to mitigate the encryption keys problem. But the laches argument presumes that Ms. McCarthy should have known more and better than they did once she read it in 2023 and come immediately to court. That's inverted. They're the ones that have the affirmative legal duty, and she's entitled to rely on them performing their affirmative legal duties correctly. It does not fall on her, and so I think that's inverted, and I think they have unclean hands charging her with laches, and in turn, there's no evidence of gross laches, no evidence that she laid around and, you know, tried to spring it on them. The issue was presented by Mr. Olsen to the Secretary's general counsel back in March of this year, and still they did nothing.

The -- we have asked for relief in the form of an order to compel them to bring the system in compliance with the certification requirements. They did not make the argument that that was impossible or infeasible for 2024. That argument has not been made. Maybe they'll make it in their case, if we get there, but they have not made that argument.

What if it is? What if it is? Well, is that same thing true for future elections after that? '25? '26? '28? I should think not. And if it is -- presents a practical problem for them to bring these systems into compliance in time for 2024, we've asked for what we call in the complaints interim and mitigating relief in the form of transparency measures, and I would say, you know, to be fair about it, that our witnesses described some additional things that could or should be done that we didn't identify in our pleading. And all of that would be good, not just what we asked for in the pleading, but specifically the things that Mr. Cotton described.

Those are not big burdens on election officials. The system -- we've got P-cap devices, those are not part of the Dominion system. That's not maintained by Dominion, but the logging can be -- they can change what gets logged. They can produce system logs, that's maintained normally. They can produce ballot images. Those are part of the process, and they can produce the cast vote record. Those are all already there, just give them to us. That will be -- it's not going to be perfect. It's not going to solve the problem entirely, but it will mitigate the problem that we have that's an urgent problem that needs to be addressed and that needs to be fixed. And the fact that -- if those mitigation measures are applied, it will serve as a deterrent, because a bad actor will know that more scrutiny is being applied, and that will have a beneficial effect. And these transparency measures will bring additional confidence to the public.

Why did we bring this case? Because we want this problem fixed. And if the Secretary had fixed it himself, we wouldn't have had to file it.

THE COURT: All right.

MS. YOUNG: May I be briefly heard just on that last point about remedies?

You know, we've had both shifting legal theories, you know, they started saying it was ministerial and now they're saying it's discretionary -- abuse of discretion, but what I haven't heard is a really cogent and clear expression of what the remedies should be. He says you should just order them to bring it into compliance --

THE COURT: I think there's quite a few things laid out in the petition, so that's what I'm using as my, kind of, point of reference.

MS. YOUNG: So, you know, I'd like to ask before you enter any kind of an order to consider what that would actually mean, because I'm certainly not sure what that would mean. In two weeks? What is it that they're asking the Secretary to actually do? You know, is it fix the system or throw out the system?

THE COURT: And I see these more, Ms. Young, as that would be a discussion we'd have if they get past your directed verdict. I don't see those as --

MS. YOUNG: But it does wrap into the directed verdict analysis, because if you can't simply order somebody to do their duty under a statute, then it's not a proper mandamus case.

I will remind you that in terms of the relief post-election, we do have a fully-litigated case pending in the Northern District. That tells you that there are adequate legal remedies out there where many of these issues may end up being decided in that forum. But, you know, if the suggestion is that the Secretary should just, you know, simply order the counties to toss out all the machines, that would be a violation of a number of legal duties that expressly were placed upon the Secretary and county superintendents by the legislature. So, you know, the remedy, I think, really illustrates why mandamus is not the right place for us to be right now.

Thanks.

THE COURT: All right. Thank you Ms. Young. All right. So based -- I know I initially had indicated that we would reconvene

Wednesday, but I think kind of in light of some of the other things that Ms. Young has brought up and some of the other cases that are active this week that I think her presence and attention will be needed elsewhere, and so also just with our own conflicts here on this docket I don't think we'd be able to come back this week, so next week would be the earliest.

I recognize the kind of time sensitive nature of the decision here, so my intention is to have a decision for you on the directed verdict by the end of the week, which I'll just file by written order on the docket. And depending on the results of that, if we need to come back and reschedule something, I'll start working logistics with the parties from there.

MR. MacDOUGALD: On scheduling, and I confess I do not have a leave of absence filed in this case, but I'm going to Europe between the 10th and the 23rd with my wife and --

THE COURT: We'll just reconvene in Paris.

MR. MacDOUGALD: And they do have Zoom from there, so --

THE COURT: Understood. We can work that out through Zoom.

Anything else we need to handle today?

MR. MacDOUGALD: No, other than thank you very much.

THE COURT: Okay. Take care.

(Whereupon the matter was adjourned at 4:31 p.m.)

DISCLOSURE

I, WHITNEY S. GUYNES, CCR, (WSG Reporting, LLC) do hereby disclose pursuant to Article 10.B of the Rules and Regulations of the Board of Court Reporting of the Judicial Council of Georgia, that I was contacted by the party taking the deposition to provide court reporting services for this deposition, and there is no contract that is prohibited by O.C.G.A. 15-14-37(a) and (b) or Article 7(c) of the Rules and Regulations of the Board for the taking of this deposition.

There is no contract to provide reporting services between WSG Reporting, LLC or any person with whom I have a principal and agency relationship nor any attorney at law in this action, party to this action, or party having a financial interest in this action.

Any and all financial arrangements beyond my usual and customary rates have been disclosed and offered to all parties.

Whitney S. Guynes

Whitney S. Guynes, CCR B-1897
October 3, 2024

CERTIFICATE

GEORGIA:

DEKALB COUNTY

I hereby certify that the total transcript, pages 5 through 309, represent a true, complete, and correct transcript of the proceedings taken down by me in the case aforesaid (and exhibits admitted, if applicable); that the foregoing transcript is a true and correct record of the evidence given to the best of my ability.

The above certification is expressly withdrawn upon the disassembly or photocopying of the foregoing transcript, unless said disassembly or photocopying is done under the auspices of myself, and the signature and original seal is attached thereto.

I further certify that I am not a relative or employee or attorney of any party, nor am I financially interested in the outcome of the actions.

This the 3rd day of October, 2024.

CERTIFIED COURT REPORTER
STATE OF GEORGIA
1776
B-1897

Whitney S. Guynes

Whitney S. Guynes, CCR B-1897

FIRM DISCLOSURE

Pursuant to Article 10B of the Rules and Regulations of the Board of Court Reporting of the Judicial Council of Georgia, I make the following disclosures:

WSG Reporting, LLC is not disqualified for a relationship of interest under the provisions of O.C.G.A. Section 9-11-28(c)

WSG Reporting, LLC will not be taking this deposition under any contract that is prohibited by O.C.G.A. Section 15-14-37(a) and (b)

WSG Reporting LLC has no exclusive contract to provide reporting services with any party to the case, any counsel in the case, or any reporter or reporting agency from whom a referral might have been made to cover this deposition.

WSG Reporting, LLC will charge its usual and customary rate to all parties in the case and a financial discount will not be given to any party to this litigation.
Date: October 04, 2024

____
WHITNEY S. GUYNES, CCR
WSG REPORTING