EXHIBIT INDEX

Petition for Reexamination – Dominion Democracy Suite 5.5A

Filed with Georgia Secretary of State – June 2, 2026

Exhibit A – Statutory Provisions: Full texts or key excerpts of O.C.G.A. §§ 21-2-368, 21-2-300, 21-2-498, 21-2-500, 21-2-52, 21-2-379, 21-2-334, and 21-2-281.

Exhibit B – Senate Bill 189 (2024) (QR-code tabulation ban effective July 1, 2026) and records confirming failure of 2026 delay/funding legislation.

Exhibit C – Independent Vulnerability Expert Reports, including Prof. J. Alex Halderman's Security Analysis of Georgia's ImageCast X.

Exhibit D – Open-records summaries and filings documenting non-preservation of ballot images and system logs.

Exhibit E – Statements from county election officials warning of logistical impossibility and chaos due to the July 1, 2026 deadline.

Exhibit F – Declaration of Clay U. Parikh (expert witness; former VSTL tester) analyzing actual 2020 Georgia county election databases (Appling, Bibb, Jones, Telfair) and identifying plaintext encryption keys and passwords.

Exhibit G – Dominion D-Suite 5.5A Test Plan and Test Report (GA DVS5_5A r1.pdf), showing limited incremental testing and Pennsylvania-specific modifications only.

Exhibit H – Ballot Assure Report "Global Password" (June 23, 2024) by Phillip Davis, documenting the hard-coded "dvscorp08!" password in Dominion Democracy Suite systems and Georgia county databases.

Exhibit I – Pro V&V Georgia State Certification Test Report for D-Suite 5.5-A (August 7, 2019) – showing limited testing scope and acknowledged memory lockup issue on ICP scanners.

All exhibits are attached and incorporated by reference.

Exhibit A – Statutory Provisions

O.C.G.A. §§ 21-2-368, 21-2-300, 21-2-498, 21-2-500, 21-2-52, 21-2-379, 21-2-334, and 21-2-281

Section 21-2-368 - Review of manufacturer's systems by Secretary of State; appointment and compensation of examiners; revocation of approval; written verification and certification prior to election or primary; penalties; conflicts of interest.

(This section shows the statutory authority for seeking recertification of the optical scanning voting system.)

(a) Any person or organization owning, manufacturing, or selling, or being interested in the manufacture or sale of, any optical scanning voting system may request the Secretary of State to examine the optical scanning voting system. **Any ten or more electors of this state may, at any time, request the Secretary of State to reexamine any optical scanning voting system previously examined and approved by him or her.** Before any such examination or reexamination, the person, persons, or organization requesting such examination or reexamination shall pay to the Secretary of State the reasonable expenses of such examination. The Secretary of State may, at any time, in his or her discretion, reexamine any optical scanning voting system.

(b) ...

(c) No kind of optical scanning voting system not so approved shall be used at any primary or election and **if, upon the reexamination of any optical scanning voting system previously approved, it shall appear that the optical scanning voting system so reexamined can no longer be safely or accurately used by electors at primaries or elections as provided in this chapter because of any problem concerning its ability to accurately record or tabulate votes, the approval of the same shall immediately be revoked by the Secretary of State;** and no such optical scanning voting system shall thereafter be purchased for use or be used in this state.

Exhibit A – Statutory Provisions

Section 21-2-300 - Provision of new voting equipment by state; uniform system using ballot scanners; pilot programs; county obligations; use of physical ballots

(This section of the law specifies that the electors voting choices be in a format readable by the elector. Currently, the voting system reads the QR code to record your selections.)

(a)

(1) The equipment used for casting and counting votes in county, state, and federal elections shall be the same in each county in this state and shall be provided to each county by the state, as determined by the Secretary of State.

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

Exhibit A - Statutory Provisions

Section 21-2-498(b) - Precertification tabulation audits; risk-limiting audits

(This section of the law specifies that audits be performed by manual inspection of the actual ballots, not ballot images or printouts of the digital image – the paper official ballots.)

(b) Local election superintendents shall conduct precertification risk-limiting audits on selected contests following any election, special election, election runoff, special election runoff, primary, special primary, primary runoff, or special primary runoff with presidential, United States Senate, or state-wide contests in accordance with requirements set forth by rule or regulation of the State Election Board. **Audits performed under this Code section shall be conducted by manual inspection of random samples of the paper official ballots.** (not the digital image or print out of the digital image)

Exhibit A - Statutory Provisions

Section 21-2-500 - Delivery of voting materials; presentation to grand jury in certain cases; preservation and destruction; destruction of unused ballots

(The Dominion Democracy Suite 5.5A system tabulates votes using digital ballot images (not just the physical paper). For any meaningful recount, audit, or verification to occur, those ballot images and the associated system logs must be preserved. § 21-2-500 (and § 21-2-52) impose a clear legal duty on county superintendents and the Secretary of State to keep these records. Open-records responses and filings (Exhibit D) show that many counties — often with Dominion assistance — have routinely failed to preserve the ballot images or system logs. Without those preserved records, it is impossible to:

1. *Perform a true risk-limiting audit under § 21-2-498,*
2. *Verify that the machine tabulation matched voter intent,*
3. *Conduct a meaningful recount*

This is therefore a direct "problem concerning the system's ability to accurately record or tabulate votes" - the exact statutory trigger for revocation under § 21-2-368.)

(a) Immediately upon completing the returns required by this article, in the case of elections other than municipal elections, the superintendent shall deliver in sealed containers to the clerk of the superior court or, if designated by the clerk of the superior court, to the county records manager or other office or officer under the jurisdiction of a county governing authority which maintains or is responsible for records, as provided in Code Section 50-18-99, the used and void ballots and the stubs of all ballots used; one copy of the oaths of poll officers; and one copy of each numbered list of voters, tally paper, voting machine paper proof sheet, and return sheet involved in the primary or election. In addition, the superintendent shall deliver copies of the voting machine ballot labels, computer chips containing ballot

Exhibit A - Statutory Provisions

tabulation programs, copies of computer records of ballot design, and similar items or an electronic record of the program by which votes are to be recorded or

Exhibit A - Statutory Provisions

tabulated, which is captured prior to the election, and which is stored on some alternative medium such as a CD-ROM or floppy disk simultaneously with the programming of the PROM or other memory storage device. **The clerk, county records manager, or the office or officer designated by the clerk shall hold such ballots and other documents under seal, unless otherwise directed by the superior court, for at least 24 months, after which time they shall be presented to the grand jury for inspection at its next meeting. Such ballots and other documents shall be preserved in the office of the clerk, county records manager, or officer designated by the clerk until the adjournment of such grand jury**, and then they may be destroyed, unless otherwise provided by order of the superior court.

Exhibit A - Statutory Provisions

Section 21-2-52 - Preservation of primary and election records

(This statute is the state-level counterpart to § 21-2-500 (which applies to county superintendents). Together they impose a clear legal duty on both the counties and the Secretary of State to preserve all primary and election documents for at least 24 months.

In the context of the Dominion Democracy Suite 5.5A system:

The system generates digital ballot images and system logs that are essential to tabulation, audits, and recounts.

These digital records qualify as "election documents."

Open-records responses and filings (Exhibit D) document that in 2020 (and in some cases later), Fulton County and multiple other counties failed to retain all original ballot images. Because the Secretary of State's office is the ultimate custodian for statewide records, § 21-2-52 makes this a statewide preservation failure under the Secretary's own responsibility.

Without preserved images and logs, meaningful verification, audits under § 21-2-498, or recounts are impossible. That constitutes a problem concerning the system's ability to accurately record or tabulate votes, a trigger for revocation under § 21-2-368.

The current system (as operated) does not produce or allow the legally required auditable records and thus Dominion Democracy Suite 5.5A cannot be deemed "safely and accurately used.")

All primary and election documents in the office of the Secretary of State shall be preserved therein for a period of at least 24 months; and then the same may be destroyed unless otherwise provided by law.

Exhibit A - Statutory Provisions

Section 21-2-379 - Arrangements for appropriate ballots when use of optical scanning voting systems impracticable

> *(This statute explicitly recognizes that there will be situations where the optical scanning system cannot be used and provides the lawful pathway to switch to hand-marked paper ballots. Our requested relief is not only reasonable but is expressly contemplated by the Georgia Election Code.*
>
> *Secretary of State should revoke approval of the Dominion Democracy Suite 5.5A system and direct counties, per Georgia Law, to prepare for hand-marked paper ballots. O.C.G.A 21-2-379 gives each county superintendent (and, by extension, the Secretary of State) the legal authority to use hand marked paper ballots when the optical scanning system becomes "impracticable.")*

Paraphrased: "If… the use of optical scanning voting systems is not possible or practicable… the superintendent may arrange to have the voting… conducted by any other lawful method authorized in this chapter. In such cases, appropriate ballots shall be printed…" *full section below:*

Full Code section:

If a method of nomination or election for any candidate or office, or of voting on any question is prescribed by law, in which the use of optical scanning voting systems is not possible or practicable, or in case, at any primary or election, the number of candidates seeking nomination or nominated for any office renders the use of optical scanning voting systems for such office at such primary or election impracticable, or if, for any other reason, at any primary or election the use of optical scanning voting systems wholly or in part is not practicable, the superintendent may arrange to have the voting for such candidates or offices or for such questions conducted by any other lawful method authorized in this chapter. In such cases, appropriate ballots shall be printed for such candidates, offices, or questions, and the primary or election shall be conducted by the poll officers, and the ballots shall be counted and return thereof made in the manner required by law for such method.

Exhibit A - Statutory Provisions

Section 21-2-334 - Voting by paper ballot when use of voting machine impossible or impracticable

This statute provides additional statutory support from the general voting-machine fallback rules. Together with 21-2-379, they reinforce that the legislature has already contemplated and authorized exactly what to do once the system is found to be impracticable.

If a method of nomination or election for any candidate or office, or of voting on any question is prescribed by law, in which the use of voting machines is not possible or practicable, or in case, at any primary or election, the number of candidates seeking nomination or nominated for any office renders the use of voting machines for such office at such primary or election impracticable, or if, for any other reason, at any primary or election the use of voting machines wholly or in part is not practicable, the superintendent may arrange to have the voting for such candidates or offices or for such questions conducted by paper ballots. In such cases, paper ballots shall be printed for such candidates, offices, or questions, and the primary or election shall be conducted by the poll officers, and the ballots shall be counted and return thereof made in the manner required by law for such nominations, offices, or questions, insofar as paper ballots are used.

Exhibit A - Statutory Provisions

Section 21-2-281 - Voting by paper ballot when use of voting equipment impossible or impracticable

This section reinforces the use of paper ballots when use of the voting equipment is impracticable.

In any primary or election in which the use of voting equipment is impossible or impracticable, for the reasons set out in Code Section 21-2-334, the primary or election may be conducted by paper ballot in the manner provided in Code Section 21-2-334.

Exhibit B – Senate Bill 189 (2024)

Senate Bill 189 (2024) – QR-Code Tabulation Ban (effective July 1, 2026) and Records Confirming Failure of 2026 Delay/Funding Legislation

This exhibit contains the 2024 Georgia law that prohibits ballot scanners from relying on QR codes or bar codes for tabulation. The human-readable text or machine marks on the ballot must constitute the official vote. It also includes records showing that attempts to delay the ban or fund replacement equipment failed, meaning the July 1, 2026 deadline remains in effect. Highlighted sections directly support Ground 1 of the petition.

Link to 2024 SB 189 : https://www.legis.ga.gov/legislation/64471

Prohibition on QR codes / coding for tabulation: "…scanners may not rely on a QR code, bar code, or similar coding to count ballots. The text portion of the ballot shall constitute the official vote for tabulation, recounts, and audits."

Effective date: This Act shall become effective on July 1, 2026.

> *Senate Bill 189 passed and specified that only the text portion of the ballot shall be used to tabulate the vote, not the QR code. The QR code was to be removed by July 1, 2026.*

Title and enactment page of Senate Bill 189 (2024), the legislation that bans reliance on QR-code tabulation.

595 **SECTION 13.**

596 (a) This section and Sections 12 and 14 of this Act shall become effective upon its approval
597 by the Governor or upon its becoming law without such approval.
598 (b) Sections 1, 2, 3, 3.1, 5, 8, 10, and 11 of this Act shall become effective on July 1, 2024.
599 (c) Sections 4, 6, and 9 of this Act shall become effective on January 1, 2025.
600 (d) Section 7 of this Act shall become effective on July 1, 2026.

Exhibit B – Senate Bill 189 (2024)

24 LC 47 3110S

SECTION 7.

Said chapter is further amended in Code Section 21-2-379.23, relating to requirements for ballot display, role of Secretary of State, and printed paper ballot controls during recount, by revising subsection (d) as follows:

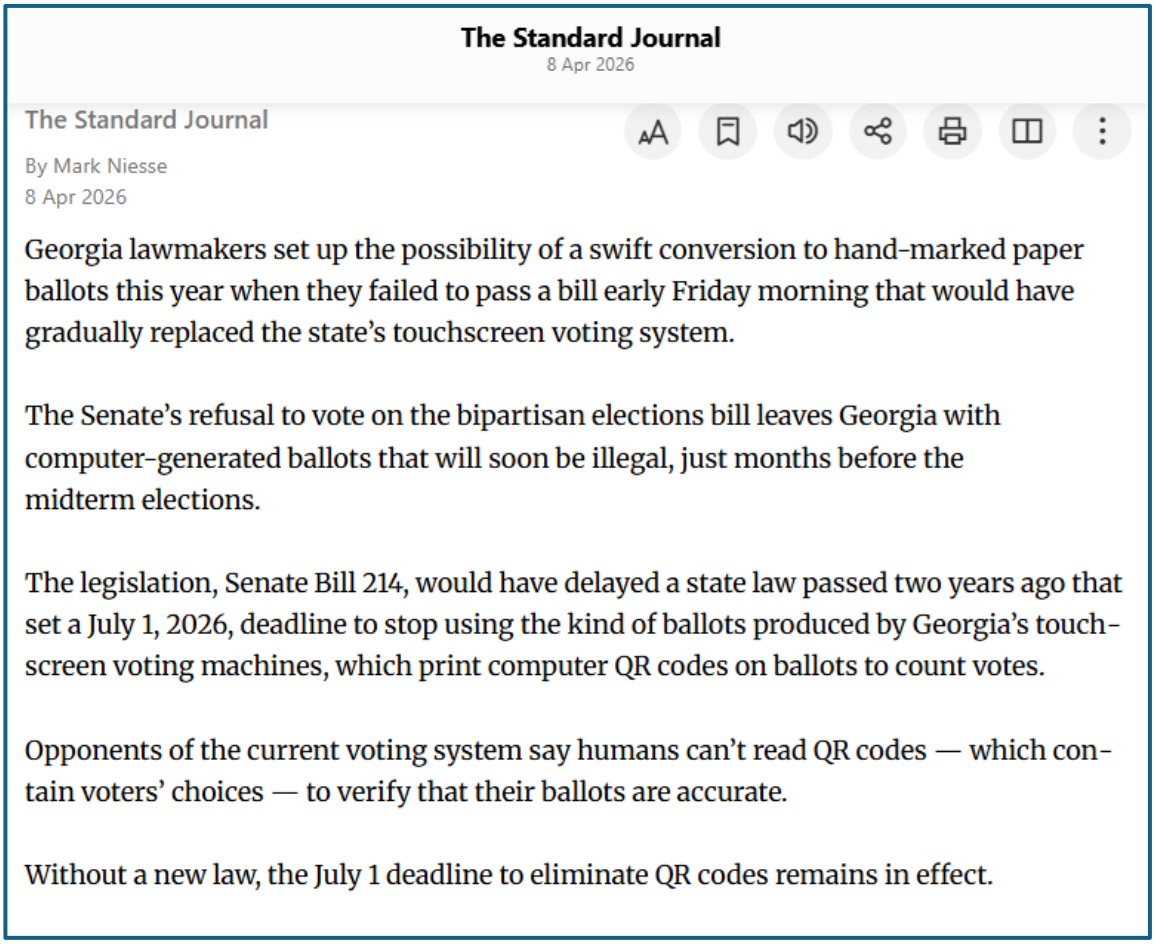
"(d) The text portion of the paper ballot marked and printed by the electronic ballot marker indicating the elector's selection shall constitute the official ballot and shall ~~be used for, and govern the result in,~~ constitute the official vote for purposes of vote tabulation, any recount conducted pursuant to Code Section 21-2-495, and any audit conducted pursuant to Code Section 21-2-498. The official tabulation count of any ballot scanner shall be based upon the text portion or the machine mark, provided that such mark clearly denotes the elector's selection and does not use a QR code, bar code, or similar coding, of such ballots and not any machine coding that may be printed on such ballots."

Key provision of SB 189 prohibiting scanners from relying on QR codes, bar codes, or similar coding. The text portion or machine marks on ballots produced by ballot marking

Exhibit B – Senate Bill 189 (2024)

The 2026 regular legislative session ended in early April 2026 without passing any delay or funding bill for the QR-code ban in Senate Bill 189 (2024).

Senate Bill 214 (2026), which would have delayed the QR-code ban until 2028 and provided funding/procurement direction, passed the House but was never taken up by the Senate before the 2026 session adjourned. A special session has been called, and the governor will likely force his own bill to delay removal in contravention to Georgia Law. Source: https://www.pressreader.com/usa/the-standard-journal/20260408/281548002449599



The Standard Journal
8 Apr 2026

The Standard Journal

By Mark Niesse
8 Apr 2026

Georgia lawmakers set up the possibility of a swift conversion to hand-marked paper ballots this year when they failed to pass a bill early Friday morning that would have gradually replaced the state's touchscreen voting system.

The Senate's refusal to vote on the bipartisan elections bill leaves Georgia with computer-generated ballots that will soon be illegal, just months before the midterm elections.

The legislation, Senate Bill 214, would have delayed a state law passed two years ago that set a July 1, 2026, deadline to stop using the kind of ballots produced by Georgia's touch-screen voting machines, which print computer QR codes on ballots to count votes.

Opponents of the current voting system say humans can't read QR codes — which contain voters' choices — to verify that their ballots are accurate.

Without a new law, the July 1 deadline to eliminate QR codes remains in effect.

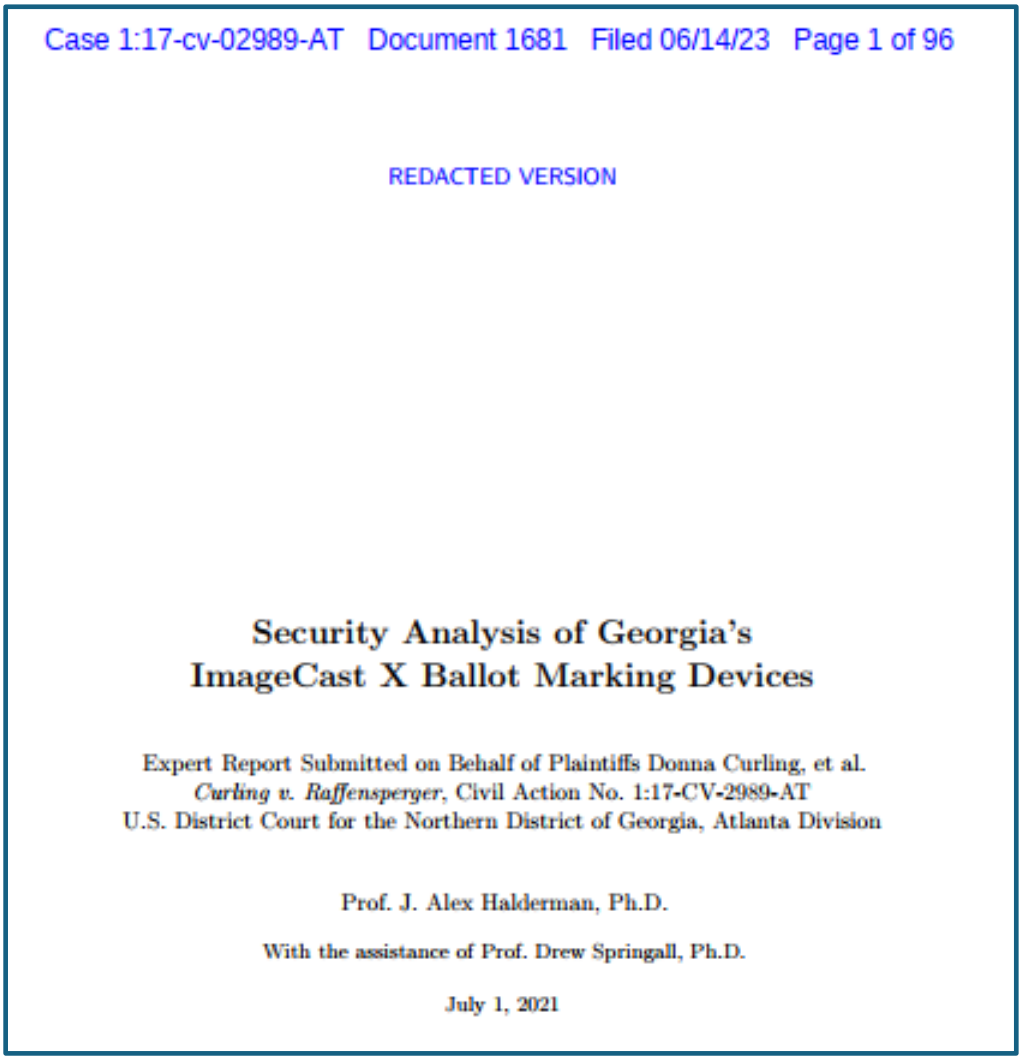
Media confirms failure of 2026 delay or funding legislation, meaning the QR-code tabulation ban will take effect as scheduled on July 1, 2026.

Exhibit C – Prof. Halderman Security Analysis

Independent Vulnerability Expert Reports, including Prof. J. Alex Halderman's Security Analysis of Georgia's ImageCast X

This exhibit contains expert demonstrations of undetectable manipulation vulnerabilities in the Dominion ImageCast X Ballot Marking Device used in Georgia. Highlighted sections show how a small change in code can allow an attacker to alter votes without detection, along with USB and memory-card exploits that bypass all security controls.

Excerpts below with official 96-page court-filed copy from Curling v. Raffensperger link here**:**
https://storage.courtlistener.com/recap/gov.uscourts.gand.240678/gov.uscourts.gand.240678.1681.0.pdf



Case 1:17-cv-02989-AT Document 1681 Filed 06/14/23 Page 1 of 96

REDACTED VERSION

Security Analysis of Georgia's ImageCast X Ballot Marking Devices

Expert Report Submitted on Behalf of Plaintiffs Donna Curling, et al.
Curling v. Raffensperger, Civil Action No. 1:17-CV-2989-AT
U.S. District Court for the Northern District of Georgia, Atlanta Division

Prof. J. Alex Halderman, Ph.D.

With the assistance of Prof. Drew Springall, Ph.D.

July 1, 2021

Exhibit C – Prof. Halderman Security Analysis

My technical findings leave Georgia voters with greatly diminished grounds to be confident that the votes they cast on the ICX BMD are secured, that their votes will be counted correctly, or that any future elections conducted using Georgia's universal-BMD system will be reasonably secure from attack and produce the correct results. No grand conspiracies would be necessary to commit large-scale fraud, but rather only moderate technical skills of the kind that attackers who

5.1 Decoding Ballot QR Codes

Dominion's documentation claims that the QR codes are encrypted [19, § 2.6.1.1], and, at least as recently as January 2021, Secretary of State Chief Operating Officer Gabriel Sterling has repeated this claim to the media as a security feature of Georgia's voting system [91]. In actuality, as I testified last year, no part of the QR codes is encrypted [40, ¶ 37–40]. While voters have no practical way to read or verify the votes encoded in the QR codes, they can be decoded by attackers and can be replaced or manipulated to steal voters' votes.

REDACTED VERSION

most robust risk-limiting audit can only assess an election outcome; it cannot evaluate whether individual votes counted as intended.

– The ICX's vulnerabilities also make it possible for an attacker to compromise the auditability of the ballots, by altering both the QR codes and the human readable text. Such cheating could not be detected by an RLA or a hand count, since all records of the voter's intent would be wrong. The only practical way to discover such an attack would be if enough voters reviewed their ballots,

Principal Findings (pages 4–7): Prof. Halderman details critical vulnerabilities in Georgia's ImageCast X that allow undetectable manipulation of votes, including altering QR codes,

Exhibit C – Prof. Halderman Security Analysis

Despite this use of a MAC, attackers can manipulate ICX QR codes through several means to alter recorded votes or cast fraudulent votes. The ICX QR code design as used in Georgia has a serious weakness: the codes do not contain a serial number or other unique identifier, so, for a given ballot design, all QR codes that contain identical votes are indistinguishable, including having identical MACs. As a consequence, there is no mechanism for detecting *duplicate* QR codes. This enables two important attacks:

Copying Ballots A copy of a genuine ICX ballot will be indistinguishable from a second genuine ICX ballot with the same votes. In tests, the ICP accepted ballots copied using an office photocopier (see Section 11.1). This could allow a variety of ballot-box stuffing attacks.

– The critical vulnerabilities in the ICX—and the wide variety of lesser but still serious security issues—indicate that it was developed without sufficient attention to security during design, software engineering, and testing. The resulting system architecture is brittle; small mistakes can lead to complete exploitation. Likewise, previous security testing efforts as part of federal and state certification processes appear not to have uncovered the critical problems I found. This suggests that either the ICX's vulnerabilities run deep or that earlier testing was superficial. In my professional experience, secure systems tend to result from development and testing processes that integrate careful consideration of security from their inception. In my view, it would be extremely difficult to retrofit security into a system that was not initially produced with such a process.

Principal Findings (pages 4–7): Prof. Halderman details critical vulnerabilities in Georgia's ImageCast X that allow undetectable manipulation of votes, including altering QR codes,

Exhibit C – Prof. Halderman Security Analysis

5.2 Defeating QR Code Authentication

Issue: *ICX QR codes are not protected against "replay" attacks, so copies of valid QR codes will be accepted as genuine.*

As an authentication mechanism, the QR code contains a cryptographic message authentication code (MAC) computed using the HMAC-SHA256 algorithm. A MAC is a value (a number) calculated based on an input and a secret key. Without knowing the key, it is infeasible to calculate the correct MAC for a modified input. In a given election, the ICX and ballot scanner have copies of the same key. Whenever an ICX generates a QR code, it uses this key to calculate the MAC of the ballot data. When a scanner reads the QR code, it extracts the data, repeats the MAC calculation using its copy of the key, and verifies that the MAC value it calculated matches the MAC in the QR code. Under the assumption that an attacker cannot discover the secret key,[8] this arrangement allows the scanners to confirm that the data in the QR code really was generated by an ICX and was not subsequently modified.[9]

– Using vulnerable ICX BMDs for all in-person voters, as Georgia does, greatly magnifies the security risks compared to jurisdictions that use hand-marked paper ballots but provide BMDs to voter upon request. When use of such BMDs is limited to a small fraction of voters, as in most other states, they are a less valuable target and less likely to be attacked at all. Even if they are successfully compromised, attackers can change at most a small fraction of votes—which, again, creates a strong disincentive to undertake the effort and risk to change any such votes.

Principal Findings (pages 4–7): Prof. Halderman details critical vulnerabilities in Georgia's ImageCast X that allow undetectable manipulation of votes, including altering QR codes,

Poll Worker Cards and PINs are distributed to every polling place and entrusted to thousands of volunteer poll workers across the state during every major election. It would be practically impossible to ensure that none of these cards could be temporarily accessed by a malicious party.

County election databases from the November 2020 and January 2021 elections shows that Georgia counties use the same cryptographic keys county-wide for each election. This means that if a single Poll Worker Card and PIN anywhere in a county is temporarily accessed by an attacker, the attacker can easily obtain the keys necessary to compromise election data throughout the county.

7.4 Modifying the ICX App to Change Votes

Due to the structure of Android applications, it is relatively straightforward to make arbitrary changes to the ICX App's behavior. We used Java, a high-level programming language, to implement demonstration malicious functionality as a Java package. Using a high-level programming language is much less labor intensive than writing the malicious logic in low-level bytecode. We compiled the Java package into low-level smali instructions using the publicly available `java2smali` software tool [51] and inserted the smali files into the disassembled APK's file structure. This arrangement allows the new code to be invoked with only small, targeted changes to the original app's code.

For example, in my demonstration malware, one place where such malicious logic is injected is in the code that generates the QR code for printing. Through reverse engineering, we located the existing code that constructs the vote data that will be encoded in the QR code. Changing just two bytecode instructions in this function[13] causes it to pass the data to a function in the new Java package, giving the malicious logic an opportunity to change the data before the QR code is produced.

As a simple demonstration, I implemented malicious logic that modifies the QR code so that the vote recorded for a specific "Yes or No" contest is always "No". The logic clears the "No" bit and sets the "Yes" bit for a specific byte

[13] Specifically, the function [redacted]

34

USB and memory-card exploits (pages 39–47): Shows how an attacker with brief physical access can attach a USB device or memory card and install malware, bypassing all security controls on the ImageCast X."

Exhibit C – Prof. Halderman Security Analysis

8 Installing Malware Locally

An attacker who has access to an ICX BMD has multiple ways to install malicious software, such as the vote-stealing malware described in Section 7. In this section, I describe three separate techniques for accomplishing this that I have successfully tested with the ICX from Fulton County.

These techniques do not require any secret passwords, PINs, or keys, nor does the attacker have to open the device's chassis or break any tamper-evident seals. They only need physical access to the BMD for a few minutes. Attackers could gain such access before machines are delivered from the manufacturer, while they are in storage, while they are being prepared for use in an election, or at the polling place. As I will show, malware could potentially even be installed by regular voters, without any special level of access or technical skill.

I understand that Georgia requires the USB port doors to be closed and secured with tamper-evident seals while the machine is in use at a polling place. The kinds of tamper-evident seals typically used in election systems are known to be easily bypassed using commonly available tools [7]. However, this is unnecessary for the attacks described here, because the seals present no practical obstacle to connecting new USB devices.

USB and memory-card exploits (pages 39–47): Shows how an attacker with brief physical access can attach a USB device or memory card and install malware, bypassing all security controls on the ImageCast X."

Exhibit C – Prof. Halderman Security Analysis

8.2 "Escaping" the ICX App

Issue: *As a result of Georgia's installation of a software update in October 2020, the ICX's Android operating system settings can be accessed by attaching a USB keyboard, allowing the installation of malware.*

In October 2020, shortly before the start of early voting in the November election, Georgia installed a purportedly *de minimis* software update on its BMDs to correct a user-interface glitch. In support of Plaintiffs' opposition to this change, I testified that "in complex computerized systems like Georgia's election equipment, last-minute changes, even seemingly small ones, can introduce serious and difficult-to-foresee consequences" [41, ¶ 5]. I drew an analogy to the Boeing 737 MAX aircraft, where a small, last-minute change to correct a single problem inadvertently created a much more dangerous failure mode that reportedly led to two fatal crashes [56].

My testing shows that installing the ICX software update did indeed create a dangerous security problem. It left the BMDs in a state where anyone with physical access, including non-technical voters, could install malicious software.

8.3 Accessing a Root Shell via the Built-In Terminal App

Issue: *The ICX has a built-in Terminal Emulator app that is configured so that the user can easily obtain a command-line shell with supervisory privileges.*

After escaping kiosk mode, an attacker can easily launch any app installed on the ICX. The machine contains 20 pre-installed apps, most of which appear unnecessary for its use as a BMD. Most notably, there is a Terminal Emulator that provides access to a Linux shell, a powerful text-based user interface.

Moreover, the ICX is configured such that the Terminal Emulator user can easily obtain supervisory ("root") access privileges by simply selecting "Allow" at an on-screen prompt, shown in Figure 11. With root privileges, terminal commands can completely bypass the Android operating system's access control restrictions and make arbitrary changes to the device's data and software.

The Terminal Emulator made analysis of the device much more efficient, since I was able to easily access, control, and modify any part of the data or software. It also makes it easy for an attacker to install programs or run automated commands for malicious purposes.

USB and memory-card exploits (pages 39–47): Shows how an attacker with brief physical access can attach a USB device or memory card and install malware, bypassing all security controls on the ImageCast X."

Exhibit C – Prof. Halderman Security Analysis

8.5 Automating Malware Installation

The process described above can be completely automated, so that an attacker can install malware by attaching a single USB device to the exposed printer cable for less than two minutes. The automated process is simple and fast enough that it could potentially be carried out by a voter in the polling place.

To automate the attack, I used a device called a "Bash Bunny", which is commercially available for less than $100 [37]. A widely-used tool for penetration testing, the Bash Bunny (shown in my hand in Figure 12) looks similar to a typical USB thumb drive, but it acts simultaneously as a USB storage device and a simulated keyboard. Once attached to a target machine, it sends a pre-programmed sequence of keystrokes to execute the attacker's objectives. I prepared the Bash Bunny by copying the malicious APK to its USB storage and programming it to send keystrokes that carry out the installation process, following a sequence of operations similar to those in Section 8.4.

Once the Bash Bunny is programmed, launching the attack requires no technical skills. A voter could do so by following simple directions like these:

USB and memory-card exploits (pages 39–47): Shows how an attacker with brief physical access can attach a USB device or memory card and install malware, bypassing all security controls on the ImageCast X."

Exhibit C – Prof. Halderman Security Analysis

8.6 Local Malware Installation using a Forged Technician Card

While the attack method demonstrated above exploits the vulnerability created when the October 2020 software update was installed, there are also other means of installing malware. One is to use a forged Technician Card created using the technique described in Section 6.2, which requires no secret passwords, keys, or PINs, but only a widely available $10 Java Card with some simple programming.

By inserting a forged Technician Card like the one I created, the attacker can access the Technical Administration menu, exit the ICX App, and then proceed to install malware using essentially the same on-screen process that is used to install official software updates. As before, a Bash Bunny could be programmed to automate the necessary steps, so that malware installation could be performed quickly by anyone with brief physical access to an ICX.

8.7 Local Malware Installation via Android Safe Mode

Issue: *A local user can reboot the ICX into "Safe Mode", allowing full control of the Android operating system.*

A third method for installing malware is to exploit a publicly known security flaw in the ICX. According to a Dominion customer advisory dated January 2020, "[i]f the mechanical power button (behind the ICX door) is pressed a power down option is presented. At this point, if the power down screen button is pressed and held, the 'safe mode' option is presented" [22].

USB and memory-card exploits (pages 39–47): Shows how an attacker with brief physical access can attach a USB device or memory card and install malware, bypassing all security controls on the ImageCast X."

Exhibit C – Prof. Halderman Security Analysis

9 Installing Malware Remotely

I have described several methods by which attackers can install malware with only brief physical access to an ICX. Although these are severe vulnerabilities, the ICX is also vulnerable to an even more dangerous method of malware installation. By modifying the election definition files that election workers copy to the BMDs before each election, attackers can spread malware to them remotely, with no physical access to the individual machines. By levering this vulnerability, an attacker who infiltrates a county Election Management System (EMS) can spread malware to every ICX in the county, and infiltrating other systems could allow vote-stealing malware to be spread to all ICXs state-wide.

USB and memory-card exploits (pages 39–47): Shows how an attacker with brief physical access can attach a USB device or memory card and install malware, bypassing all security controls on the ImageCast X."

Exhibit C – Prof. Halderman Security Analysis

11.1 The ICP Accepts Photocopied Ballots

Issue: *The ICP as tested did not require ballots to be printed on security paper, and it accepted ICX ballots photocopied on normal office paper.*

Georgia uses special "security" paper stock for official ballots, including those printed by BMDs [32, 35]. However, when I tested the Fulton County ICP using ballots printed on normal copier paper, it accepted and counted them normally. I also tested scanning photocopies of BMD-printed ballots, and the ICP again accepted and counted them normally.

11.2 A Dishonest Poll Worker with Access to the ICP Memory Card can Deanonymize All Voted Ballots

Issue: *The ICP tested does not encrypt ballot images stored on its memory card.*

Issue: *ICP memory cards store ballot images in the order they were cast.*

The ICP stores a complete digital image of every scanned ballot on its removable memory card, and these images are returned to the EMS for possible later review or adjudication. On the Fulton County scanner I tested, the ballot images were not encrypted, and I could easily extract them. Moreover, my testing shows that the unencrypted ballot images are stored in the order in which they were cast, potentially deanonymizing the secret ballots.

Encrypting ballot images appears to be a configuration option that jurisdictions can enable. That option was not enabled in the ICP I tested, which was purportedly configured in the same way as the scanners used during Georgia elections. In any event, even if jurisdictions were to enable this encryption option, the county-wide encryption keys can be be extracted from any ICX Poll Worker Card, given brief access to the card and PIN (see Section 6.1).

The system will accept photocopied ballots and ballots are not encrypted.

Exhibit C – Prof. Halderman Security Analysis

9.6 Conclusions

I have identified critical vulnerabilities in the ICX software that enable an attacker to remotely execute arbitrary code on the device. These vulnerabilities can be exploited by maliciously altering the election definition files that workers copy to all ICXs before every election.

Security experts consider arbitrary code execution to be one of the most dangerous classes of vulnerabilities, particularly when it can be exploited to run code with root privileges, as it can on the ICX. In 2006, Harri Hursti discovered a similar arbitrary code execution vulnerability that affected Georgia's old AccuVote TS-X DREs [45]. At the time, Defendants' expert Michael Shamos called it "the most serious security breach that's ever been discovered in a voting system" [44]. The vulnerabilities in the ICX are as or more severe.

Using these vulnerabilities, I developed functional proof-of-concept malware that automatically and invisibly installs itself on any ICX on which an infected election definition file is loaded, then manipulates voters' printed ballots to steal votes. By compromising election definition files in this way, an attacker with access to a county's EMS could spread malware to all ICXs in the county, and an attacker who infiltrated the systems that Dominion uses to prepare initial election projects for all Georgia counties could spread vote-stealing malware to every ICX used in Georgia. As I discussed in Section 3.2, even the ICX's use of a paper trail poses no obstacle to vote-stealing attacks in the vast majority of elections and contests, and malware can also evade Georgia's other technical and procedural defenses.

Conclusion and Recommendations (page 53): Prof. J. Alex Halderman concludes that Georgia's ImageCast X system cannot be considered secure for use in elections due to these undetectable vulnerabilities.

Exhibit C – Prof. Halderman Security Analysis

1.1 Principal Findings

I show that the ICX suffers from critical vulnerabilities that can be exploited to subvert all of its security mechanisms, including: user authentication, data integrity protection, access control, privilege separation, audit logs, protective counters, hash validation, and external firmware validation. I demonstrate that these vulnerabilities provide multiple routes by which attackers can install malicious software on Georgia's BMDs, either with temporary physical access or remotely from election management systems (EMSs). I explain how such malware can alter voters' votes while subverting all of the procedural protections practiced by the State, including acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs).

2. The software update that Georgia installed in October 2020 left Georgia's BMDs in a state where anyone can install malware with only brief physical access to the machines. I show that this problem can potentially be exploited in the polling place even by non-technical voters (Section 8).

3. Attackers can forge or manipulate the smart cards that the ICX uses to authenticate technicians, poll workers, and voters. Without needing any secret information, I created a counterfeit technician card that can unlock any ICX in Georgia, allowing anyone with physical access to install malware (Section 6).

4. I demonstrate that attackers can execute arbitrary code with root (supervisory) privileges by altering the election definition file that county workers copy to every BMD before each election. Attackers could exploit this to spread malware to all BMDs across a county or the entire state (Section 9).

5. The ICX contains numerous unnecessary Android applications, including a Terminal Emulator that provides a "root shell" (a supervisory command interface that overrides access controls). An attacker can alter the BMD's audit logs simply by opening them in the on-screen Text Editor application (Section 10).

6. In a given election, all BMDs and scanners in a county share the same set of cryptographic keys, which are used for authentication and to protect election results on scanner memory cards. An attacker with brief access to a single ICX or a single Poll Worker Card and PIN can obtain the county-wide keys.

Conclusion and Recommendations (page 53): Prof. J. Alex Halderman concludes that Georgia's ImageCast X system cannot be considered secure for use in elections due to these undetectable vulnerabilities.

Exhibit C – Prof. Halderman Security Analysis

1.2 Main Conclusions

On the basis of the technical findings described in this report, I reach the following conclusions:

- The ICX BMDs are not sufficiently secured against technical compromise to withstand vote-altering attacks by bad actors who are likely to attack future elections in Georgia. Adversaries with the necessary sophistication and resources to carry out attacks like those I have shown to be possible include hostile foreign governments such as Russia—which has targeted Georgia's election system in the past [49]—and domestic political actors whose close associates have recently acquired access to the same Dominion equipment that Georgia uses through audits and litigation in other jurisdictions.

- The ICX BMDs can be compromised to the same extent and as or more easily than the AccuVote TS and TS-X DREs they replaced.[3] Both systems have similar weaknesses, including readily bypassed user authentication and software validation, and susceptibility to malware that spreads from a central point to machines throughout a jurisdiction. Yet with the BMD, these vulnerabilities tend to be even easier to exploit than on the DRE system, since the ICX uses more modern and modular technology that is simpler to investigate and modify.

- Despite the addition of a paper trail, ICX malware can still change individual votes and most election outcomes without detection. Election results are determined from ballot QR codes, which malware can modify, yet voters cannot check that the QR codes match their intent, nor does the state compare them to the human-readable ballot text. Although outcome-changing fraud conducted in this manner could be detected by a risk-limiting audit, Georgia requires a risk-limiting audit of only one contest every two years, so the vast majority of elections and contests have no such assurance. And even the

Conclusion and Recommendations (page 53): Prof. J. Alex Halderman concludes that Georgia's ImageCast X system cannot be considered secure for use in elections due to these undetectable vulnerabilities.

Exhibit C – Prof. Halderman Security Analysis

Professor Halderman commented on his blog post about the report, writing: Our report explains how attackers could exploit the flaws we found to change votes or potentially even affect election outcomes in Georgia, including how they could defeat the technical and procedural protections the state has in place. While we are not aware of any evidence that the vulnerabilities have been exploited to change votes in past elections, without more precautions and mitigations, there is a serious risk that they will be exploited in the future.

The report was filed under seal on July 1, 2021 and remained confidential until today (June 14, 2023), but last year the Court allowed us to share it with CISA—the arm of DHS responsible for election infrastructure—through the agency's coordinated vulnerability disclosure (CVD) program. CISA released a security advisory in June 2022 confirming the vulnerabilities, and Dominion subsequently created updated software in response to the problems. Georgia Secretary of State Brad Raffensperger has been aware of our findings for nearly two years, but—astonishingly—he recently announced that the state will not install Dominion's security update until after the 2024 Presidential election, (he still has not done so) giving would-be adversaries another 18 months to develop and execute attacks that exploit the known-vulnerable machines.

Source: https://blog.citp.princeton.edu/2023/06/14/security-analysis-of-the-dominion-imagecast-x/)

Exhibit D – Open Records proof of non-preservation

Open-records summaries and filings documenting non-preservation of ballot images and system logs. This document includes county-by-county responses showing that Fulton County and dozens of other counties could not produce all original 2020 ballot images. It cites over 70 counties with missing or destroyed images.

37.

The Respondents did not object to the requests, and stated that they had no such records, contrary to state and federal law that requires them to be retained. No original scanned ballot images were ever produced.

Source: VoterGA Ballot Image Destruction and Ballot Preservation Petition: https://voterga.org/wp-content/uploads/2022/11/VoterGA-Ballot-Image-Destruciton-and-Ballot-Preservation_Petition.pdf

---- Forwarded Message ----
From: "Eveler, Janine" <Janine.Eveler@cobbcounty.org>
To: "ElectionsORR" <ElectionsORR@cobbcounty.org>, "Welch47" <welch47@aol.com>
Sent: Tue, Jul 27, 2021 at 9:18 AM
Subject: RE: Open Records Request

We do not have a complete record of the ballot images for the November 2020 election. Since there was no rule or law at the time requiring retention, the images were not saved. Some images are still available on memory cards or on the scanners, but the data is incomplete. Memory cards are reused each election and in many cases were overwritten. After a special request made in a December 1, 2020 Official Election Bulletin, we did send a complete set of ballot images to the Secretary of State after the November recount, so you could request the November images from the Secretary of State's office. If you want us to provide what we have, knowing they are incomplete, please let me know and we can provide you with a time and cost estimate.

Janine Eveler

Director,

Cobb County Elections & Registration

Exhibit D – Open Records proof of non-preservation

From: Scoggins, Jane <jscoggins@coweta.ga.us>
Sent: Monday, October 25, 2021 10:35 AM
To: Garland Favorito
Cc: Gay, Ashley
Subject: RE: ORR Follow Up Question

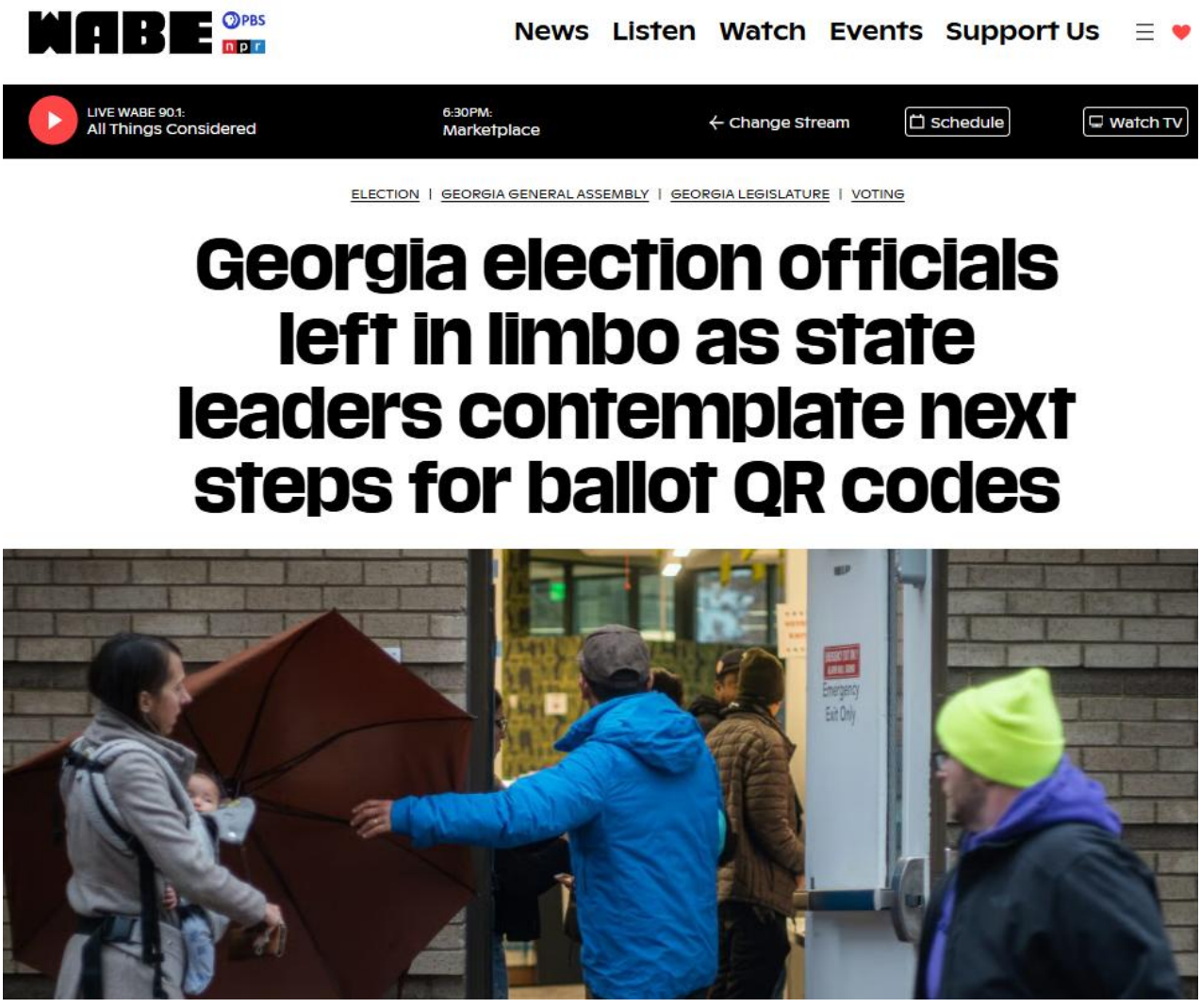
The recount ballot images are the same as the "original" ballot images. We do not have the ballot images on the server from the November 3, 2020, election.
Please let me know if you need additional information.

Jane Scoggins
Elections Director
Coweta County
22 East Broad Street
Newnan, GA 30263

Source: https://voterga.org/wp-content/uploads/2025/04/Favorito-Ballot-Image-Destruction-Affidavit-and-Exhibits.pdf

Exhibit E – Media reports on botched QR Code funding

County election officials across Georgia have publicly warned that the July 1, 2026, QR-code ban (with no delay or funding enacted) leaves them in limbo and makes proper election planning impossible."



https://www.wabe.org/georgia-election-officials-left-in-limbo-as-state-leaders-contemplate-next-steps-for-ballot-qr-codes/

Exhibit E – Media reports on botched QR Code funding

https://www.wtoc.com/2026/04/09/georgia-election-officials-raise-concerns-over-qr-code-ballot-ban-deadline/

Exhibit E – Media reports on botched QR Code funding

https://www.wrdw.com/2026/04/06/ga-lawmakers-end-session-without-fix-looming-ballot-counting-deadline/

Exhibit E – Media reports on botched QR Code funding

GEORGIA RECORDER

GOVERNMENT/POLITICS ENERGY/ENVIRONMENT EDUCATION HEALTH CRIMINAL JUSTICE CIVIL RIGHTS ELECTION 2026

ELECTION 2026 GOVERNMENT & POLITICS

Election measures capsize on the final day of Georgia's 2026 legislative session

BY: MAYA HOMAN - APRIL 3, 2026 3:05 AM

An election worker in Gwinnett County demonstrates how to insert a voter card into ballot-marking devices used by voters across Georgia. Maya Homan/Georgia Recorder

In an unexpected twist, members of the House and Senate concluded the 2026 legislative session without ending their longstanding stalemate over election policy, as Georgia hurtles toward the deadline for removing QR codes from voters' ballots without a clear solution in sight.

https://georgiarecorder.com/2026/04/03/election-measures-capsize-on-the-final-day-of-georgias-2026-legislative-session/

Exhibit F - Declaration of Expert Clay U. Parikh

Declaration of Clay U. Parikh (dated August 7, 2024).

This is a sworn expert declaration by a former Voting System Test Laboratory (VSTL) tester who personally performed security testing on Dominion voting systems. He examined actual 2020 Georgia county election databases (Appling, Bibb, Jones, and Telfair) and discovered secret encryption keys, digital certificates, and passwords stored in plain, unencrypted text — a serious violation of federal security standards and Georgia's contract with Dominion. Highlighted sections summarize the key findings

The highlighted sections summarize his key findings.

Declaration of Clay U. Parikh

I, CLAY U. PARIKH, declare under penalty of perjury that the following is true and correct:

1. I have personal knowledge of the matters set forth below and would testify competently to them if called upon to do so.

2. 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).

Page 1 – Qualifications of Clay U. Parikh, former VSTL security tester for Wyle Laboratories, NTS, and Pro V&V on EAC and state certifications.

Exhibit F - Declaration of Expert Clay U. Parikh

Declaration of Clay U. Parikh (dated August 7, 2024).

EXECUTIVE SUMMARY

8. 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.

9. 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.

Pages 2–3 – Executive Summary: Parikh identifies plaintext encryption keys, x509 certificates, and hard-coded passwords in Georgia county election databases, violating EAC, FIPS 140-2, and VVSG standards.

Exhibit F - Declaration of Expert Clay U. Parikh

Declaration of Clay U. Parikh (dated August 7, 2024).

10. 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.

11. 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

12. 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**.

Pages 4–6 – Detailed Findings: Technical explanation of the violations and screenshots from actual Georgia county databases showing secret keys stored in plain text, creating an egregious security vulnerability.

Exhibit F - Declaration of Expert Clay U. Parikh

Declaration of Clay U. Parikh (dated August 7, 2024).

13. 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.

17. 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

Pages 2–3 – Executive Summary: Parikh identifies plaintext encryption keys, x509 certificates, and hard-coded passwords in Georgia county election databases, violating EAC, FIPS 140-2, and VVSG standards.

Exhibit F - Declaration of Expert Clay U. Parikh

Declaration of Clay U. Parikh (dated August 7, 2024

11. 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.

CONCLUSION

24. 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.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 7th day of August 2024.

s/ Clay Parikh
Clay U. Parikh

Pages 4–6 – Detailed Findings: Technical explanation of the violations and screenshots from actual Georgia county databases showing secret keys stored in plain text, creating an egregious security vulnerability.

Exhibit F - Declaration of Expert Clay U. Parikh

Declaration of Clay U. Parikh (dated August 7, 2024).

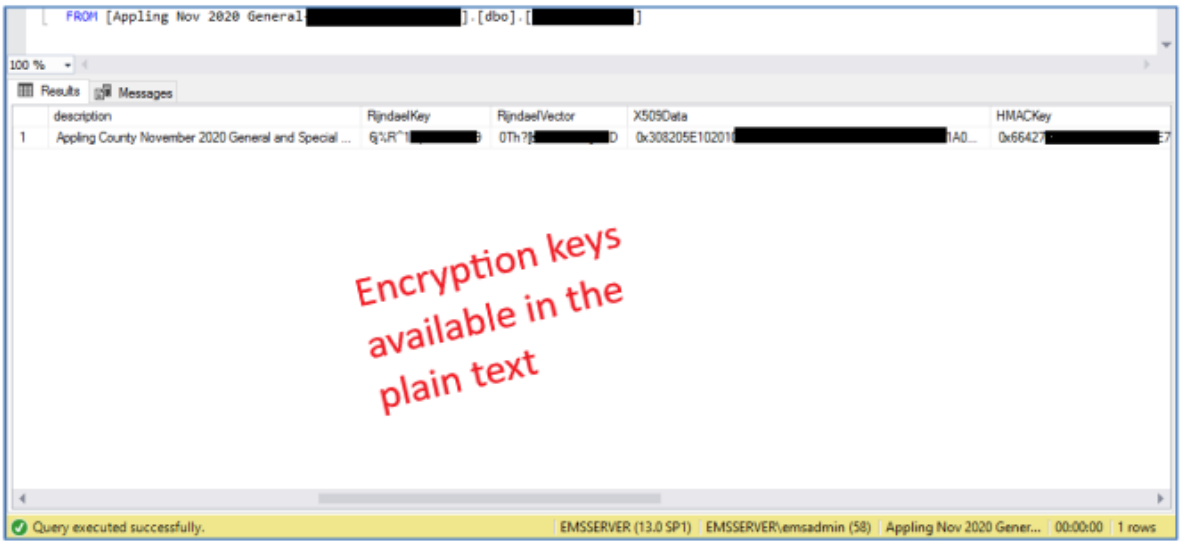


Figure A-1. Appling encryption keys

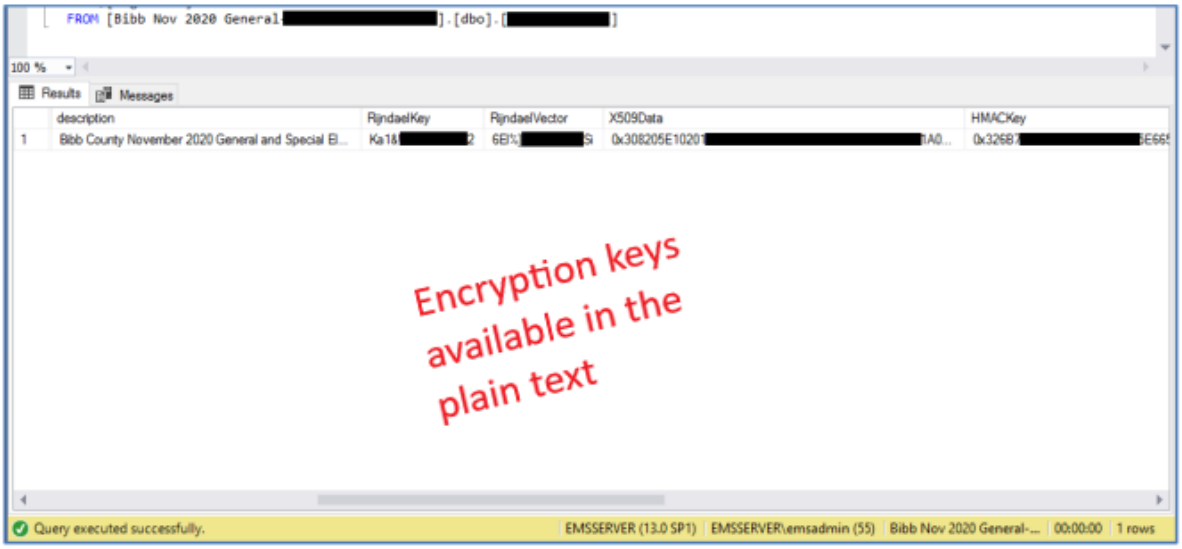


Figure A-2. Bibb encryption keys

Pages 9–12 – Exhibits A and B: Actual screenshots from Georgia county election databases (Appling, Bibb, Jones, Telfair) showing plaintext Rijndael encryption keys, x509 certificates, and shared hard-coded passwords

Exhibit F - Declaration of Expert Clay U. Parikh

Declaration of Clay U. Parikh (dated August 7, 2024).

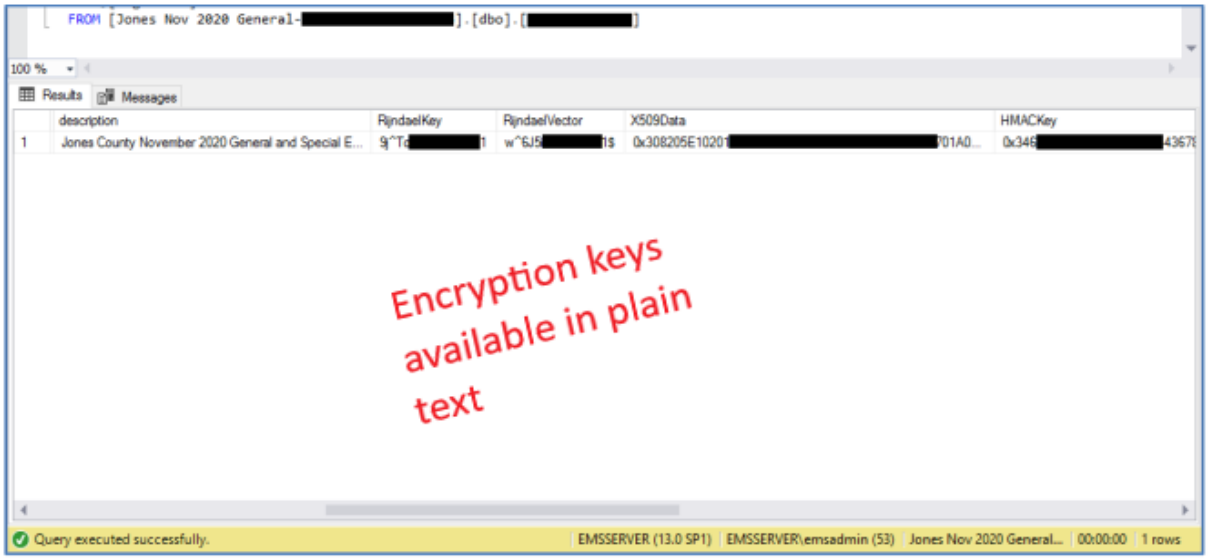


Figure A-3. Jones encryption keys

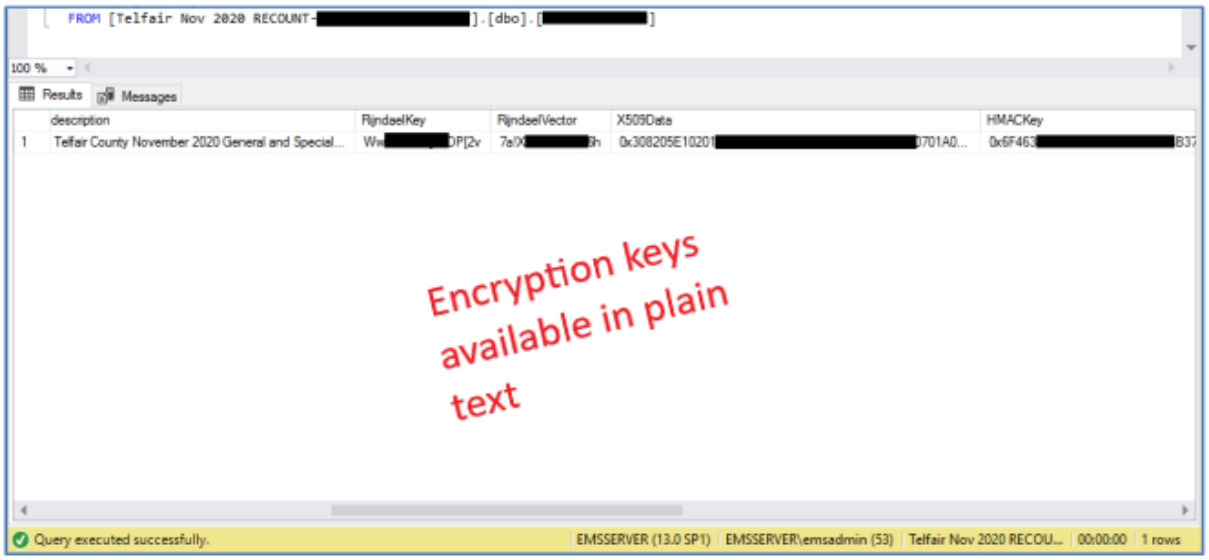


Figure A-4. Telfair encryption keys

Pages 9–12 – Exhibits A and B: Actual screenshots from Georgia county election databases (Appling, Bibb, Jones, Telfair) showing plaintext Rijndael encryption keys, x509 certificates, and shared hard-coded passwords

Full 12-page sworn declaration is attached for reference.

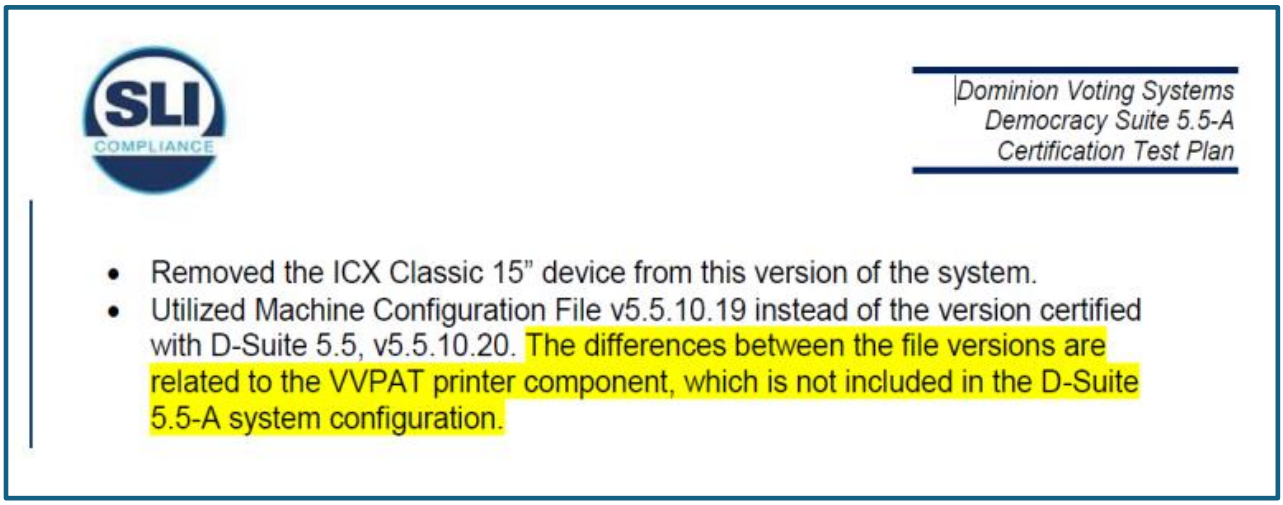
Exhibit G – Dominion Test Plan

Dominion D-Suite 5.5A Test Plan. This exhibit is the preliminary test plan used for certification of the Dominion Democracy Suite 5.5A system. The highlighted portions show that testing was limited in scope and consisted only of incremental modifications from the prior D-Suite 5.5 version — primarily Pennsylvania-specific changes. Source-code review was performed only on the modified modules.

Highlighted sections demonstrate:

- The system was treated as a modification of the previous version (not a full new system).
- Source code review was restricted to changed portions only.
- The testing plan focused on limited engineering changes required by Pennsylvania.

Title page (above) showing this is the 'DVS 5.5A Test Plan' and (below) that differences are limited to the VVPAT printer component (not part of the Georgia configuration).



1.4.1 Project Schedule

The following schedule outlines the expected timeline for this project.

Task Name	Start	Finish
DVS D-Suite 5.5-A	**Mon 11/12/18**	**Wed 1/30/19**
Test Readiness Review (TRR)	**Mon 11/12/18**	**Fri 11/16/18**
Project Initiation	**Tue 11/20/18**	**Wed 11/21/18**
Client Deliverables	**Tue 11/20/18**	**Wed 11/21/18**
Receive and Setup Voting System Hardware	**Mon 11/12/18**	**Wed 11/14/18**
Documentation Review	**Wed 11/21/18**	**Wed 11/21/18**
Source Code Review	**Wed 11/21/18**	**Wed 11/21/18**
Test Plan	**Fri 11/30/18**	**Tue 12/11/18**
Create Test Plan	Fri 11/30/18	Fri 11/30/18
Submit Test Plan for EAC Review	Fri 11/30/18	Tue 12/11/18

Project schedule highlighting that only 'Source Code Review' and 'Documentation Review' were performed for the modified modules.

1 Introduction, System Identification and Overview

SLI Compliance is submitting this report as a summary of the certification testing efforts for the **Dominion Voting Systems (Dominion) Democracy Suite 5.5-A (D-Suite 5.5-A)** voting system, as detailed in the section System Identification. The purpose of this document is to provide an overview of the certification testing effort and the findings of the testing effort for **Dominion D-Suite 5.5-A** voting system.

The purpose of the **Dominion D-Suite 5.5-A** voting system release is to make modifications to the **D-Suite 5.5** voting system as required by the State of Pennsylvania.

This effort included documentation review of the Technical Data Package, source code review, and testing of the **Dominion Voting Systems (Dominion) Democracy Suite 5.5-A (D-Suite 5.5-A)** voting system. Testing consisted of the development of a test plan, managing system configurations, executing test suites of functional and system levels tests based on the system's functionality, and analysis of results. The review and testing was performed at SLI's Wheat Ridge, Colorado facility.

Purpose statement: 'The purpose of the Dominion D-Suite 5.5-A voting system release is to make modifications to the D-Suite 5.5 voting system as required by the State of Pennsylvania.

1.4.3 Engineering Changes

The following engineering changes occurred to software and hardware for the **Dominion D-Suite 5.5-A** voting system.

Table 6 – Engineering Changes 5 changes to the ICX were listed

Engineering Changes section noting only 5 changes to the ICX and that only modified modules were reviewed.

or errors in documentation were identified to **Dominion** in a Discrepancy Report for resolution or comment. This Discrepancy Report can be found in Attachment C.

All PCA source code reviews were conducted in accordance with Vol. 1 Section 5.2 and Vol. 2 Section 5 of the EAC VVSG 1.0, to demonstrate that the system meets the requirements. A total of 376 lines of code were modified in this release. The delivered code base was compared to the previous code base from **Dominion D-Suite 5.5,** with only modified modules being reviewed.

No inconsistencies or errors were found in the modified source code.

Full document is attached for reference.

Exhibit H – Phillip Davis Expert Opinion

Ballot Assure Report "Global Password" (June 23, 2024) by Phillip Davis.

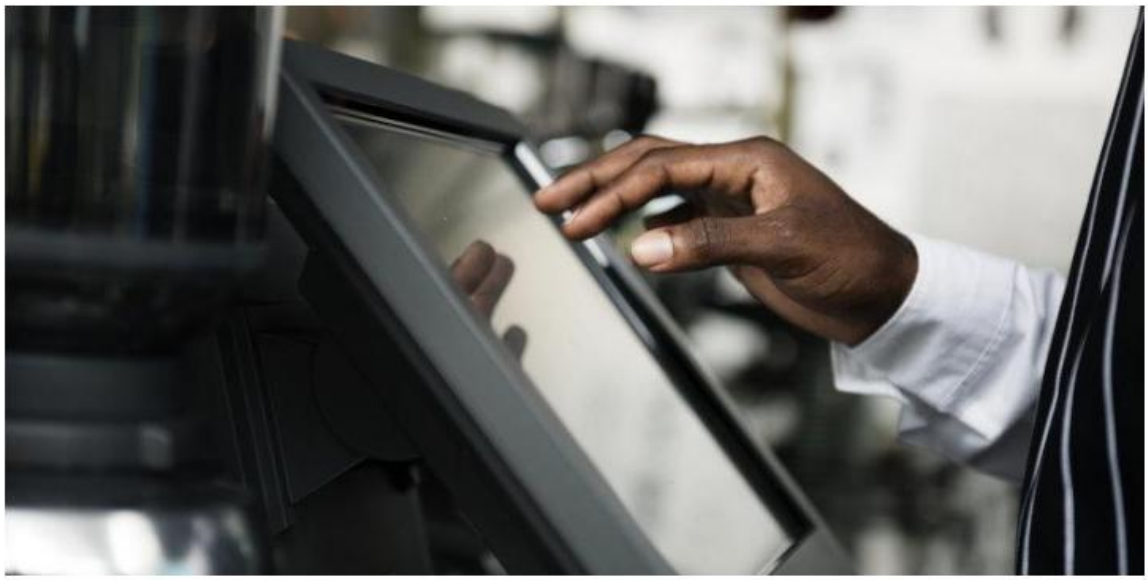
This report documents the existence of a hard-coded password "dvscorp08!" in Dominion Democracy Suite systems and confirms that this exact password is present in actual Georgia county election databases. Highlighted sections show this long-standing security defect that allows unauthorized high-privilege access to election systems and undermines the security of the Dominion Democracy Suite 5.5A.

Security Analysis

Administrative Passwords

14 Year Old Hard Coded Passwords

Jun 23, 2024 By Phillip Davis



Executive Summary

This report uncovers critical security vulnerabilities in the voting systems used in various states across the United States. Through comprehensive analysis, significant issues were identified, particularly with the use of hard-coded passwords embedded in the source code. These vulnerabilities raise serious concerns about the overall security and integrity of these systems.

Source: https://www.ballotassure.com/Reports/Security/GlobalPassword

Exhibit H – Phillip Davis Expert Opinion

Key findings include:

1. **Hard-Coded Passwords**: The discovery of a hard-coded password that has remained unchanged since at **least 2010**. This password is embedded directly in multiple points in the source code, making it easily exploitable by anyone with access to the code.
2. **High-Level Access Vulnerabilities**: User accounts with high-level administrative privileges, such as **MRE Super Admin**, are inadequately protected. These accounts likely have extensive access rights, making their compromise particularly dangerous.
3. **Widespread Use of Global Passwords**: The same global password is used across multiple voting systems in different states, including Georgia, Arizona, New Mexico, and Michigan. This uniformity creates a single point of failure, increasing the risk of widespread unauthorized access.
4. **Weak Password Management Practices**: Passwords are not unique per user within counties, meaning multiple users share the same password. This further compromises security, making it easier for unauthorized users to gain access.

Key findings: A hard-coded global password has been embedded in Dominion Democracy Suite source code since at least 2010, inadequate security protections for MRE Super Admins, and widely known passwords.

> `dvscorp08!`

This is a significant issue. The password **dvscorp08!** was hard-coded directly into the source files at least 14 years ago. One would assume that this problem has been fixed by now, or at the very least, the password has been changed. Unfortunately, that assumption would be incorrect.

Confirmation that the password 'dvscorp08!' (and its SHA-256 hash) appears in Georgia county election databases."

Exhibit H – Phillip Davis Expert Opinion

Results | Messages

	username	firstName	lastName	password	salt
1	Techadvisor	State of	Georgia	0x08A1312BF6EEFD5856D0072BA452A2E80B32FC6A614E574470075FEFA8319A7B	0x
2	Admin	State of	Georgia	0x08A1312BF6EEFD5856D0072BA452A2E80B32FC6A614E574470075FEFA8319A7B	0x
3	county	Telfair	County	0x1C8138C179AA1F5B8A45E862A34FCAA24D7E844A1D1F24D8CE89BD4938D49F2E	0x
4	RTRAdmin	Telfair	County	0x1C8138C179AA1F5B8A45E862A34FCAA24D7E844A1D1F24D8CE89BD4938D49F2E	0x
5	SAdmin	MRESuper	Admin	0x6166A73E5165E844EA8A384F35616CC848C0CBA784CC93340340C9ECEF986384	0x
6	MRO01	MRO	M01	0x6166A73E5165E844EA8A384F35616CC848C0CBA784CC93340340C9ECEF986384	0x
7	ROAdmin	Return Office	Admin	0x6166A73E5165E844EA8A384F35616CC848C0CBA784CC93340340C9ECEF986384	0x

— Telfair County, Georgia - AppUser Database Table

The use of a global password across different machines and the repetition of passwords among users within the same county highlights a critical weakness in the password management system. Ideally, each user should have a unique password to ensure that if one account is compromised, it does not jeopardize others. Furthermore, the presence of a globally used password that can be used across multiple systems creates a single point of failure, making it easier for an attacker to gain widespread access.

This weak password management system not only increases the risk of unauthorized access but also makes it difficult to track and manage potential security breaches. Each user having a unique password is a fundamental security practice that enhances accountability and reduces the risk of widespread breaches. The continued reliance on global and non-unique passwords reveals a need for a comprehensive overhaul of the current security practices to protect sensitive election data effectively.

Confirmation that the password ‘dvscorp08!’ (and its SHA-256 hash) appears in Georgia county election databases and other states.

Exhibit H – Phillip Davis Expert Opinion

```
SELECT Username, FirstName, LastName, Password, Salt
  FROM [Appling County].[dbo].[AppUser]
  ORDER BY password
```

150 %

Results | Messages

	Username	FirstName	LastName	Password	Salt
1	county	Appling	County	0x36CE681E2A6E4175D14A6157973848EA781699C4FE59426BA72DAA9F43FC3A91	0x
2	RTRAdmin	Appling	County	0x36CE681E2A6E4175D14A6157973848EA781699C4FE59426BA72DAA9F43FC3A91	0x
3	SAdmin	MRESuper	Admin	0x6166A73E5165E844EA8A384F35616CC848C0CBA784CC93340340C9ECEF986384	0x
4	MRO01	MRO	M01	0x6166A73E5165E844EA8A384F35616CC848C0CBA784CC93340340C9ECEF986384	0x
5	ROAdmin	Return Office	Admin	0x6166A73E5165E844EA8A384F35616CC848C0CBA784CC93340340C9ECEF986384	0x
6	Admin	State of	Georgia	0xC97922D8B68F7F39259C2EDA397313E09639BF175E9A27B61FFD2794A6A2EF52	0x
7	Techadvisor	State of	Georgia	0xC97922D8B68F7F39259C2EDA397313E09639BF175E9A27B61FFD2794A6A2EF52	0x

— Appling County, Georgia - AppUser Database Table

These globally used passwords are stored in this database table for the following usernames:

Security implications: The password is used for high-privilege accounts (SAdmin, ROAdmin, etc.) and stored in plaintext or unsalted hashes, creating a serious single point of failure for election system security."

Who uses this password?

This password is embedded in the source code, and its hash can be easily reversed. But where is it used? Frankly, it could be in every DVS system that has been in operation for years.

I have found this password being used in at least seven database systems across **Georgia**, **Arizona**, and **New Mexico**. Cyber Ninjas also discovered the use of this password in **Antrim County, Michigan**.

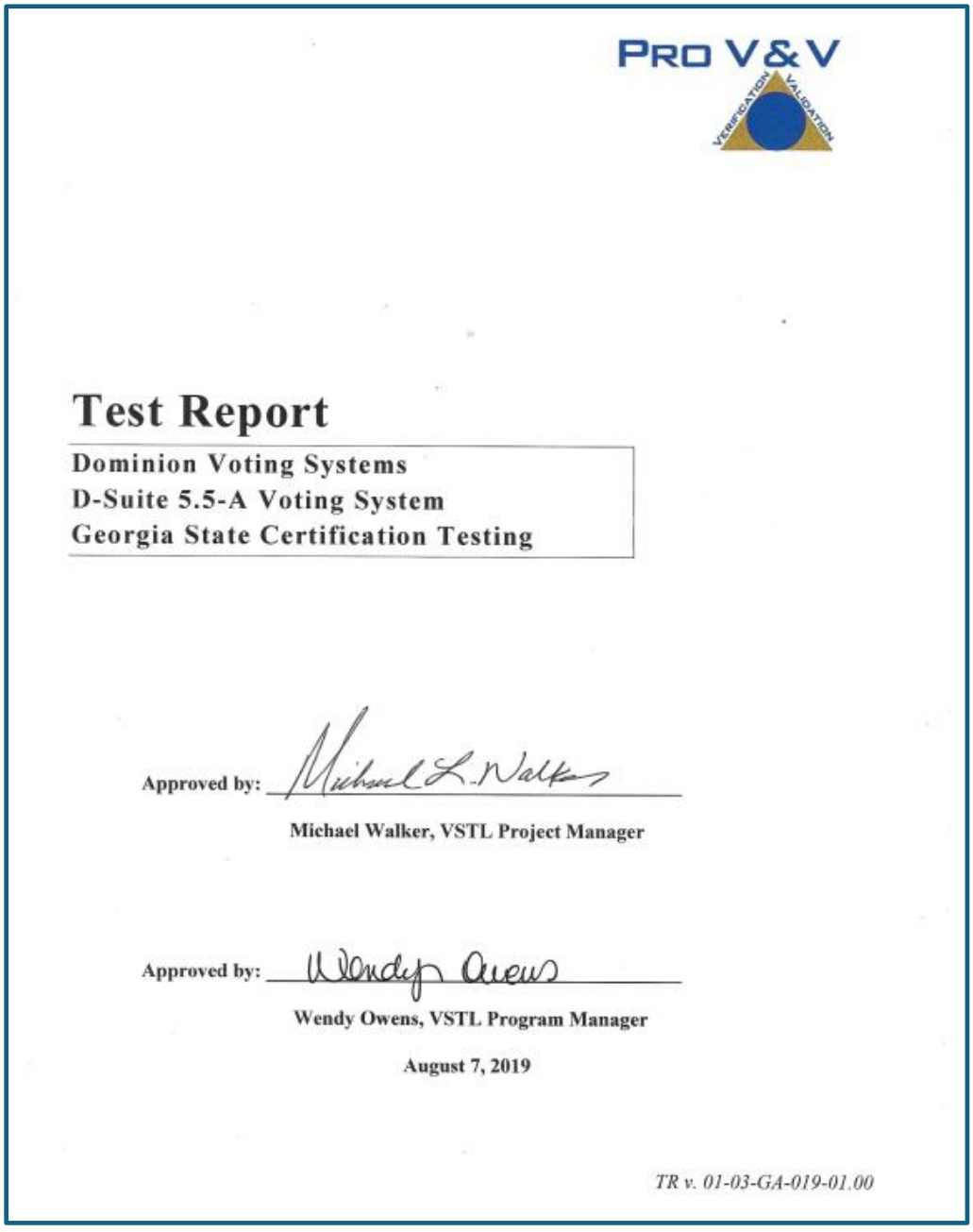
Summary

This article highlights significant security vulnerabilities in the voting systems used in various states across the United States. One of the most alarming issues is the use of a hard-coded globally used password embedded in the source code, which has remained unchanged since at least 2010. This password has been discovered in multiple database systems across Georgia, Arizona, and New Mexico, and even in Antrim County, Michigan, as revealed by the Cyber Ninjas.

Confirmation that the password 'dvscorp08!' (and its SHA-256 hash) appears in Georgia county election databases Telfair and Appling Counites. (Davis only had access to 4 Georgia Counties and it was in all of them.

Exhibit I – Final Dominion Test Report

Official Pro V&V Georgia State Certification Test Report for D-Suite 5.5-A (August 7, 2019). This is the final signed report confirming the testing was narrow in scope and testing was limited and incremental - not a full security review of the Georgia system.



PRO V&V

VERIFICATION VALIDATION

Test Report

Dominion Voting Systems
D-Suite 5.5-A Voting System
Georgia State Certification Testing

Approved by: Michael L. Walker

Michael Walker, VSTL Project Manager

Approved by: Wendy Owens

Wendy Owens, VSTL Program Manager

August 7, 2019

TR v. 01-03-GA-019-01.00

Title page of the official Pro V&V Georgia State Certification Test Report for Dominion D-Suite 5.5-A (August 7, 2019).

Exhibit I – Final Dominion Test Report

1 INTRODUCTION

The purpose of this Test Report is to document the procedures that Pro V&V, Inc. followed to perform certification testing of the Dominion Voting Systems D-Suite 5.5-A Voting System Voting System to the requirements set forth for voting systems in the State of Georgia Election Systems Certification Program.

1.5 Scope

The state certification test was not intended to result in exhaustive tests of system hardware and software attributes; these are evaluated during federal compliance testing. However, all system

2 TEST CANDIDATE

The D-Suite 5.5-A Voting System is a paper-based optical scan voting system consisting of the following major components: The Election Management System (EMS), the ImageCast Central (ICC), the ImageCast Precinct (ICP), and the ImageCast X (ICX) BMD. The D-Suite 5.5-A Voting System configuration is a modification from the EAC approved D-Suite 5.0 system configuration. The D-Suite 5.5-A Voting System will be configured with the KNOWiNK Pollpad which utilizes the ePulse Epoll data management system, for voter registration purposes.

Page 4 – The report explicitly states that the D-Suite 5.5-A system 'is a modification from the EAC approved D-Suite 5.0 system configuration.' This shows the testing was incremental and limited to changes from the previously certified version.

Exhibit I – Final Dominion Test Report

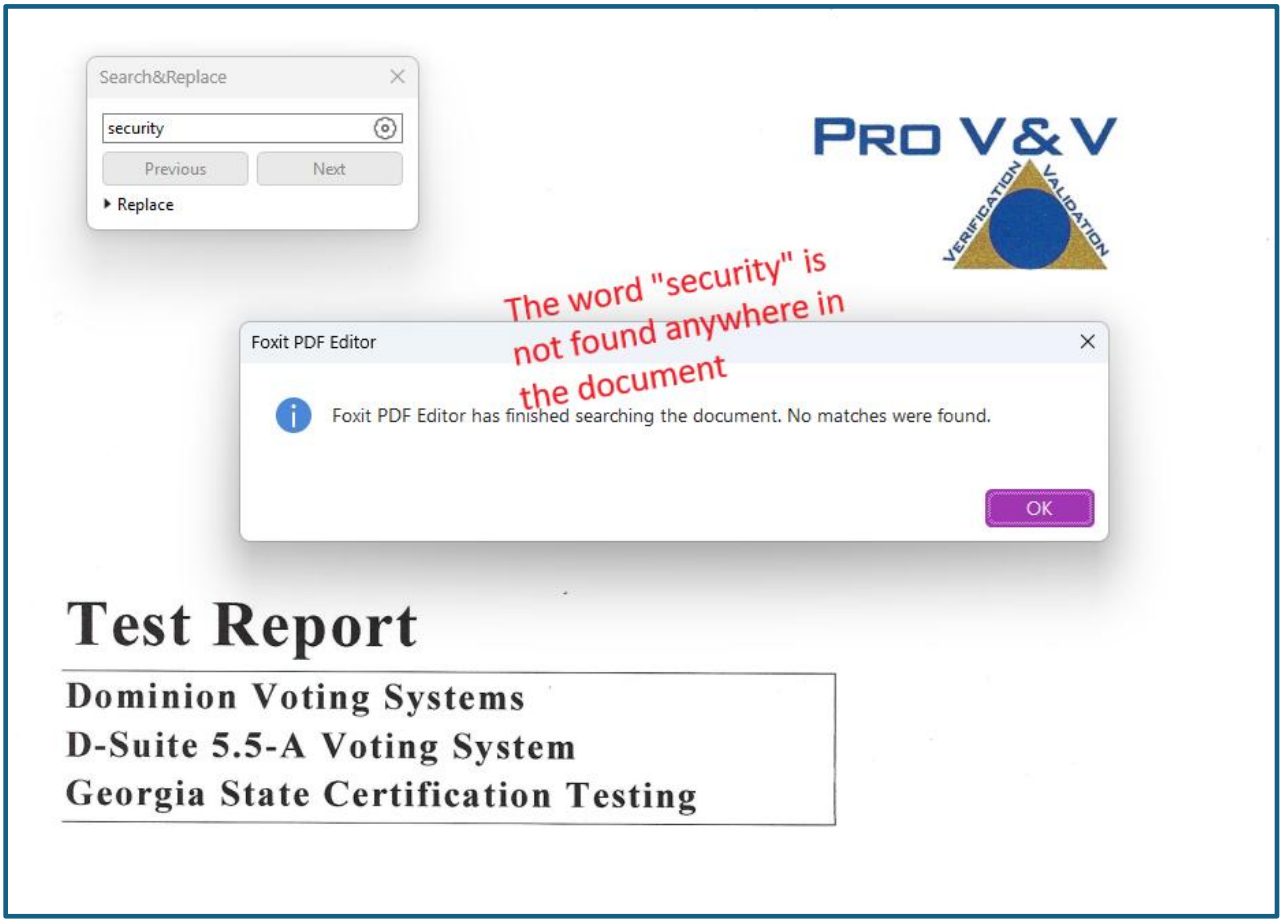
Summary Findings

The D-Suite 5.5-A system successfully passed the Accuracy Test. It was noted during test performance that the ICP under test experienced a memory lockup after scanning approximately 4500 ballots. The issue was presented to Dominion for resolution. Dominion provided the following analysis of the issue:

The ICP uClinux operating system does not have a memory management unit (MMU) and, as such, it can be susceptible to memory fragmentation. The memory allocation services within the ICP application are designed to minimize the effects of memory fragmentation. However, if the ICP scans a large number of ballots (over 4000), without any power cycle, it can experience a situation where the allocation of a large amount of memory can fail at the Operating System level due to memory fragmentation across the RAM. This situation produces an error message on the ICP which requires the Poll Worker to power cycle the unit, as documented. Once restarted, the ICP can continue processing ballots without issue. All ballots scanned and counted prior to the power cycle are still retained by the unit; there is no loss in data.

Page 15 – Summary Findings: The ImageCast Precinct (ICP) scanner experienced a memory lockup after scanning approximately 4,500 ballots, requiring a poll-worker power cycle. Dominion's analysis and Pro V&V's verification are documented here.

Exhibit I – Final Dominion Test Report



The word “security” cannot be found anywhere in the testing document.

Exhibit I – Final Dominion Test Report

The Georgia system is explicitly described as a modification of a previously certified version.

- The report repeatedly calls D-Suite 5.5-A a modification of the earlier D-Suite 5.5 (or 5.0) system, not a full new system.
- Purpose of the release: "to make modifications to the D-Suite 5.5 voting system as required by the State of Pennsylvania."

The source code review was restricted to only the changed parts (meaning, we did not test what Pennsylvania had already tested).

- "The delivered code base was compared to the previous code base from Dominion D-Suite 5.5, with only modified modules being reviewed."

Only a very small number of changes were made

- "5 changes to the ICX were listed."
- The testing focused on those specific engineering changes, not the entire system.

The testing was built on prior VSTL testing of the baseline version

- "VSTL testing has been performed on the version previous to the Dominion D-Suite 5.5-A voting system. The previous version of this system, D-Suite 5.5, is EAC certified, and will serve as the source code base for this evaluation."

Full 27-page official Pro V&V Georgia State Certification Test Report is attached for reference.