Suzy Patriot
100 Downtown Dr.
Hopeulikit, GA 30461
suzp@gmail.com
912-777-7777

July 28, 2022

Gina Public, Clerk
Any County Superior Court
Hopeulikit, GA 30458

Re: Open Records Request for Georgia 5/24/22 Primary Election Returns

Dear Ms. Public,

I am among citizens who regularly monitor the justice system and matters related to Georgia elections by purposeful exercise of our First Amendment rights. My lawful request is regarding the 5/24/22 primary election returns of Any County that were delivered to you by the Elections Supervisor and secured for storage retention by your required seal as lawful custodian per (*Attachment A* seal document if you have it).

It is your legal obligation to "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..." under O.C.G.A. § 21-2-500. As you are aware, these include federal election returns, so also appear to engage the federal oversight of the United States Election Assistance Commissions (EAC) and its rules implementing provisions of the Freedom of Information Act (FOIA). FOIA strongly favors broad government transparency and is an origin document of our current Georgia Open Records Act.

My lawful request engages no statutory or court-ordered exemptions under federal or state law, and are therefore public records open for inspection and copy per O.C.G.A. § 50-18-71. I need no reason to request these records. However, a significant document chart of legal reasoning for my request is in *Attachment B*.

You are a distinct agency with duty in Georgia under the Open Records Act, O.C.G.A. § 50-18-70. And, all definitions regarding election returns per O.C.G.A. § 21-2-2 can be found in *Attachment C*.

AS A UNITED STATES CITIZEN OF THE STATE OF GEORGIA, I AM HEREBY FILING AN OPEN RECORDS REQUEST FOR :

100% of the authentic, voter-inspected, verifiable official paper ballots of the Any County 5/24/22 Georgia Primary Election. In form, I ask that you remit, by timely response, black and white photocopies of the following categories of ballots, amounting to no less than 100%: cast absentee, provisional, challenged, voided, and used ballots.

NOTE: These paper ballots are election documents clearly considered part of the voting system audit loop, according to the Office of the Georgia Secretary of State (SoS), https://securevotega.com/. All records should be clearly marked and banded in the seven recently-filed and retrievable cartons in your storage area, and I plan to provide you manpower for the consolidative copy and inspection process. Please provide me with a cost quote for fair value fees associated with fulfillment.

To protect everyone involved in the election oversight process, the authentic, voter-inspected, verifiable official paper ballots bear no personally identifiable information per O.C.G.A. § 21-2-280. Most citizens marked their official ballots on a touchscreen (ballot marking device) using their finger or stylus. The machine-printed ballot papers generated by our markings contain our original intellectual property with human-readable text. Other citizens, including military, absentee, and provisional voters completed paper forms using writing utensils. All voters should have personally inspected the human-readable text on their ballots prior to casting them. All Any county primary voters surrendered these documents, which cumulatively contain our sacred county elective will, to the Any County Elections Department for temporary safekeeping per O.C.G.A. § 50-18-73.

Any QR-code scanning or manipulation of any type that occurred to our authentic, voter-inspected, verifiable official paper ballots as part of either physical handling or further electronic ballot 'interpretation' after ballots were cast was not verifiable by voters. Therefore, **ballot scanner or 'tabulating machine' output is not part of this open records request**. This 'interpreted ballot image' output of the voting system is a 'Cast Vote Records Snapshot' of the Dominion electronic system per NIST Cast Vote Records Common Data Format Specification, V. 1.0 (2019). They are inauthentic and inadequate for our purposes.

Additionally, law indicates you are a Constitutional Officer, and part of a division of the Georgia Court System. I believe that you are also a county employee. As such, you are personally subject to requirements under the Georgia Open Records Act, which covers records transferred to agencies "for storage" per O.C.G.A. § 50-18-70(b)(1). Your duty to remit open records as Clerk of Court per Title 50, Chapter 18, Article 4 is explicitly stated in O.C.G.A. § 15-6-60.1(b). It also appears that the authority of superior court judges "to exercise all other powers necessarily appertaining to their jurisdiction or which may be granted them by law" involves matters of open government access regarding documents that the court possesses as custodian per O.C.G.A. § 15-6-9(8).

The public is highly interested in these election returns and is aware of numerous problems in this particular primary election. Your county Elections Department shall have received a request for these ballots on 5/24 from VoterGA, long before they went under your seal. They failed to remit.

Of particular concern, there is a new Federal Advisory Warning on the electronic voting system used in Bulloch County and statewide. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ICSA-22-154-01 released an Advisory on 6/3/22 entitled *Vulnerabilities Affecting Dominion Voting Systems Democracy Suite Image Cast X,* which you can find in *Attachment D.* This advisory broadly recommended that mitigations be implemented to prevent and/or detect exploitation of these vulnerabilities. A relevant mitigation reads, "Conduct rigorous post-election tabulation audits of the human-readable portions of physical ballots and paper records, to include reviewing ballot chains of custody and conducting voter/ballot reconciliation procedures." Citizens will conduct this specific mitigation per their personal duty and right of access to public records.

Additionally, it may be useful to know that authentic, voter-inspected, verifiable **official ballot records from the 5/24 primary election have now been unsealed in other Georgia counties for copy and**

inspection under Georgia law. To support open government, the law even states that "Any agency or person who provides access to information in good faith shall not be liable in any action on account of such decision" per O.C.G.A. § 50-18-73. Local jurisdictions are enlightening to the infringements of state government employees and public officials in this matter of access and striving to protect themselves O.C.G.A. § 1-3-6.

Finally, I ask that if the court intends to keep all requested materials under seal in their entirety, which would be another violation of Georgia law from our perspective, we request entry of a publicly available order justifying that measure. See *United States v. Hubbard, 650 F 2d 293, 317-322 (D.C. Circuit 1980).* In the absence of such an order, the public has no meaningful ability to evaluate the adequacy of the reasons for the secrecy and (if appropriate) challenge it through a motion to intervene.

This matter is of urgent public interest. I anticipate your reply, and am willing to accept calls from your office to address any questions.

Respectfully,

Suzy Patriot
Any County Citizen
912-777-7777

CC:
Judge
Judge
Judge

Attachments:
A - Any County 5/24/22 Primary Election Chain of Custody Document (optional)
B - Chart of Legal Reasoning
C - Definitions
D - DHS / CISA Federal Advisory

BOOK 2022G PAGE 308

FILED
BULLOCH COUNTY
CLERK'S OFFICE
2022 JUN 15 P 1:57
Heather Bowles McNeal
CLERK OF COURT

Election Items Turned Over to Superior Court Clerk of Court for Election Held on May 24, 2022

- Consolidated Return Sheets
- Summary Report
- One copy of accumulated results tape
- Ballot Recap Sheet
- Poll Pad Recap Sheet
- Provisional Ballot Recap Sheet
- Absentee Ballot Recap Sheet
- Touchscreen Recap Sheets (Advance Voting & Election Day)
- Scanner Recap Sheets (Advance Voting & Election Day with zero tapes)
- Numbered List of Voters
- Statement of Votes Cast (SOVC)
- Absentee numbered list of voters
- Absentee ballot oath envelopes
- Cast absentee, provisional, challenged, voided, and used ballots
- Copy of thumb drive of official results
- Electronic file with Ballot Images, Vote Totals, and a copy of the Consolidated Returns from the Election Management System
- Chain of Custody form - Poll Manager
- Chain of Custody form - Technician Purposes
- Yellow copy of Manager Oath
- Yellow copy of the Clerks Oath
- Yellow copy of the Consolidated Assistance Oath

Total number of boxes with the above listed items turned over to the Clerk of Superior Court: 7

On 6/15/22, I, Shontay Jones, Bulloch County Elections Supervisor, turned over 7 boxes of Election Records to Heather McNeal, Clerk of Superior Court of Bulloch County.

Shontay Jones

On 6/15/22, I, Heather McNeal, received 7 boxes of Election Records from Shontay Jones.

Heather B McNeal

ATTACHMENT B

Legal Reasoning for this Open Records Request

Fact / Assertion	Statute Excerpt	Citation
"Because public men and women are amenable 'at all times' to the people, they must conduct the public's business out in the open."	Public officials are "servants of the people."	*Davis v. City of Macon*, statement of Georgia Supreme Court Chief Justice Charles Weltner. Georgia Constitution.
Open government is essential to a free and functional representative government.	The strong public policy of this state is in favor of open government; that open government is essential to a free, open, and democratic society; and that public access to public records should be encouraged to foster confidence in government and so that the public can evaluate the expenditure of public funds and the efficient and proper functioning of its institutions…"	The Georgia Open Records Act, textual preface O.C.G.A. § 50-18-70(a)
Both the Open Meetings Act and the Open Records Act apply to all entities that are an "agency" of the state or local government in Georgia.	Relevant Agency definitions: - every department agency, board, bureau, commission, similar body of each county, city or other political subdivision of the state -every local, regional or other authority established pursuant to state law	O.C.G.A. § 50-14-5 and § 50-18-73
The starting place under Georgia law for citizens seeking to attend meetings of governmental bodies or to inspect governmental records is the presumption that the meeting and records are open.	Law declares "a strong presumption" in favor of inspection, stating that public records should be made available "without delay."	O.C.G.A. § 50-18-70(a)
I can request the ballot records from the clerk of court. That individual is the custodian as part of her agency. Remittance shall be timely.	A request made pursuant to this article may be made to the custodian of a public record orally or in writing. Agencies shall produce for inspection all records responsive to a request within a reasonable amount of time not to exceed three days of receipt of a request, [with some additional guidance.]	O.C.G.A. § 50-18-71
Under the Open Records Act, these exclusions are to be interpreted narrowly. All election records are open for public inspection and copy unless specifically excluded. Official ballots are not excluded.	This Code section shall be interpreted narrowly so as to exclude from disclosure only that portion of a public record to which an exclusion is directly applicable. It shall be the duty of the agency having custody of a record to provide all other portions of a record for public inspection or copying.	O.C.G.A. § 50-18-72(b)
Strict compliance is required. Arbitrary restriction generates violations.	District attorney's failure to cite the Code section, subsection, and paragraph, pursuant to which the state was denying the applicant's request, violated O.C.G.A. § 50-18-71(d) for which strict compliance was required.	Chua v. Johnson, 336 Ga. App. 298, 784 S.E.2d449 (2016). Annotation of O.C.G.A. § 50-18-71.
Many of the exclusions are	In May 2017, the Court of Appeals	Campaign for Accountability v.

discretionary, permitting public disclosure even when not required or specifically allowed with no legal consequences.	issued its opinion which concluded: In light of the Georgia Supreme Court's decision in Bowers, the trial court erred in ruling that KSU had the discretion to release the research correspondence in response to CFA's open record request, even if [CCRF] brought suit to enjoin the disclosure and demonstrated that the correspondence was exempt from disclosure under O.C.G.A. § 50-18-72(a)(35) or (36). The KSU Board can just say that it is releasing materials on its own volition.	Consumer Credit Research Found., 303 Ga. 828 (2018)
The law strongly leans heavily toward the citizen requester and access to public records. The court shall assess in favor of the complaining party, in most cases.	Any agency or person who provides access to information in good faith shall not be liable in any action on account of such decision.	O.C.G.A. § 50-18-73
Anyone refusing to provide timely open records access or attempts to frustrate the process shall be guilty of crime.	Anyone refusing to provide access to records not subject to exemption from this article, or refusing to provide access to such records within the time limits, or by knowingly and willingly attempting to frustrate the access to records by intentionally making records difficult to obtain or review shall be guilty of a misdemeanor punishable by a fine not to exceed $1,000.00 ($2,500 for subsequent violations).	O.C.G.A. § 50-18-74
The case of Smith V. DeKalb County is not relevant to this open records request. It specifically references an open records request filed by Mr. Smith for an election CD-ROM that had been under seal of the DeKalb Clerk of Superior Court for nearly 3 months. Smith had requested remittance from the DeKalb County Director of Voter Registration and Elections, who did not have the election returns at the time and therefore could not provide the public records. The court upheld the Secretary of State's petition for a permanent injunction prohibiting the clerk of court custodian from opening the records. The CD-ROM was also found to be excluded because it contained sensitive, proprietary information.	2022 Election Code Annotation: Sealed CD-ROM containing election information not open record subject to disclosure. Because a superior court had not ordered that its seal be lifted under O.C.G.A. § 21-2-500, a CD-ROM containing election information was by law prohibited or specifically exempted from being open to inspection by the general public and thus was not an open record subject to disclosure under O.C.G.A. § 50-18-70(b). The trial court also found that release of the CD-ROM, which contains passwords, encryption codes, and other security information, would compromise election security. It was exempted under O.C.G.A. § 50-18-72(a)(15)(A)(iv). Smith's witness claimed he could break the encryption codes.	Smith V. DeKalb County, 288Ga. App. 574 (2007). O.C.G.A. § 21-2-500
Machine-printed returns (actual paper ballots) are considered "election returns" under O.C.G.A. § 21-2-491 and in the basic legal definition existing in the field of election law. Machine-printed returns are open to public inspection.	The general returns from the various precincts which have been returned unsealed shall be open to public inspection at the office of the superintendent as soon as they are received from the chief managers.	O.C.G.A. § 21-2-491
The ballots are not under seal until	Immediately upon completing the	O.C.G.A. § 21-2-500

they are delivered to the Superior Court Clerk. Nowhere does it even mention the word “seal” until after the completion and delivery of returns to the clerk of court. A sealed container is a non-legal seal representing a lid or tape.	returns required by this article, in the case of elections other than municipal elections, the superintendent [Board of Elections and Registration or designee] shall deliver in sealed containers to the clerk of the superior court… as provided in O.C.G.A. § 50-18-99, the used and void ballots… The clerk… shall hold such ballots and other documents under seal, unless otherwise directed by the superior court, for at least 24 months…”	O.C.G.A. § 50-18-99
At the time of inspection, any person may make copies.	At the time of inspection, any person may make photographic copies or other electronic reproductions of the records using suitable portable devices brought to the place of inspection.	O.C.G.A. § 50-18-71(b)
An agency’s use of an electronic record-keeping system, such as an electronic voting system with stored digital voting data, must not erode the public’s right of access to it. Dominion system paper ballots are records created by citizen interaction with the ballot marking device (touchscreen), marked with electronic information (pixelated words and markings), and printed by a machine (printer).	An agency’s use of electronic record-keeping systems must not erode the public’s right of access to records under this article. Agencies shall produce electronic copies of, or, if the requester prefers, printouts of electronic records.	O.C.G.A. § 50-18-71(f)
None of the Dominion ballots or digital system ballot snapshots contain any private information connecting them to individual citizens.	The legislature shall provide a method, or methods, of voting at elections in such a way that not even those who count or tabulate the votes will know how any particular voter voted.	Favorito v. Handel, 285 Ga. 795, 684 S.E.2d 257 (2009). O.C.G.A. § 21-2-280
The Secure the Vote website maintained by the Georgia Secretary of State markets dozens of times that the paper ballots are an excellent feature of the new Dominion ‘paper-ballot’ system signed in contract by Brad Raffensberger (8/12/2019) and Gabriel Sterling (8/9/2019).	The Georgia State Legislature approved the purchase of a new, statewide voting system in order to replace aging, paperless election equipment dating back to 2002. The new system offers Peach State voters more modern, up-to-date technology with important security and transparency features. The new system will also produce a paper ballot to allow for verification and auditing of election results. An evaluation committee scored each applicant based on an appraisal of cost and ability to meet the state’s voting system specifications, which included accuracy, security, auditability, and ease of use for poll managers and voters. These touchscreens also produce paper-ballots for auditing and reduce paper volumes overall.	www.securethevotega.com

	The paper ballots are used for verifying and auditing results. Georgia's paper-ballot system includes: ● ImageCastX Ballot Marking Device (the touchscreen): A universal voting device with accessible options, the touchscreen operates with a printer that produces a paper ballot. ● ImageCast Precinct Polling Place Scanner: Allows ballots to be scanned, capturing ballot images for auditing/review. The new, paper-ballot system will enable Georgia to defend against cyber threats and deliver reliable election results which can be audited using paper ballots. ● Like the existing voting machines, the new machines do not connect to the Internet, which limits cybersecurity risks. They also create an auditable paper-ballot, with other enhanced review capabilities for the public. The Dominion touchscreens also produce a human-readable ballot summary for voter verification. Most tabulation systems that count paper ballots currently use a barcode to accurately and efficiently count each vote. The Dominion touchscreens also produce a human-readable ballot summary for voter verification. Plus, election officials test and affirm the security of the system prior to every election, as well as during post-election audits. While voters can be confident in the ability of the paper-ballot system to ensure trustworthy and accurate election results, Dominion will be working with the Secretary of State's office to address perceived concerns regarding use of marked ballots that feature barcodes. For example, the state can make scanned images of all ballots cast in statewide elections available, allowing anyone to do a ballot count to check the accuracy of results. Secure the Vote Office of the Secretary of State Press Release Dec 30, 2019: (ATLANTA) – Monday the Secretary of State's Office will deliver the largest shipment to metro Atlanta of equipment for Georgia's new secure paper-ballot system.	

	Secure the Vote Office of the Secretary of State Press Release Dec 30, 2019: (ATLANTA) An important aspect of the rules are procedures for maintaining the integrity of the touchscreen ballot-marking devices, known as BMDs. The rules require county poll managers to test each BMD before every election to ensure that voters' selections will be accurately printed on the ballots. Georgia is replacing its first-generation electronic voting machines with a secure paper-ballot system. Voters in the new system will make their selections by touchscreen as they have for the past 17 years, except that then they will print out their ballot and review it before casting it.	

ATTACHMENT C

Definitions per O.C.G.A. § 21-2-2

(1) "Ballot" means "official ballot" or "paper ballot" and shall include the instrument, whether paper, mechanical, or electronic, by which an elector casts his or her vote.
[Citizens cast our ballot using our finger and a computer screen or ballot marking device BMD. That machine printed out on a piece of paper that contains our original intellectual property. Anything scanning or manipulating that occurred to that piece of paper as part of ballot 'interpretation' is outside of voter custody and oversight. Ballots scanner or 'tabulating machine' output is not part of this open records request. Some individuals completed paper absentee or provisional ballots with writing utensils. I request elector verifiable paper ballot original form photocopies.]

(2.1) "Ballot scanner" means an electronic recording device which receives an elector's ballot and tabulates the votes on the ballot by its own devices; also known as a "tabulating machine."

(7) "Elector" means any person who shall possess all of the qualifications for voting now or hereafter prescribed by the laws of this state, including applicable charter provisions, and shall have registered in accordance with this chapter.

(7.1) "Electronic ballot marker" [also known as a BMD] means an electronic device that does not compute or retain votes; may integrate components such as a ballot scanner, printer, touch screen monitor, audio output, and a navigational keypad; and uses electronic technology to independently and privately mark a paper ballot at the direction of an elector, interpret ballot selections, communicate such interpretation for elector verification, and print an elector verifiable paper ballot

(18) "Official ballot" means a ballot, whether paper, mechanical, or electronic, which is furnished by the superintendent or governing authority in accordance with Code Section 21-2-280, including paper ballots that are read by ballot scanners.
[Ballot scanners are separate devices used to interpret ballots into the voting system. I am not requesting interpreted ballot output of the voting system.] NOTE: only official ballots furnished by the superintendent or governing authority shall be cast or counted in any primary or election in any precinct in which ballots are used.

Statute Describing the Official Ballot O.C.G.A. § 21-2-284.
Form of official primary ballot; attestation regarding receiving value in exchange for vote.
(a) In each primary separate official ballots shall be prepared for the political party holding the primary. At the top of each ballot shall be printed in prominent type the words "OFFICIAL PRIMARY BALLOT OF _____ PARTY FOR," followed by the name and designation of the precinct for which it is prepared and the name and date of the primar

(19.1) "Optical scanning voting system" means a system employing paper ballots on which electors cast votes with a ballot marking device or electronic ballot marker after which votes are counted by ballot scanners.

(20) "Paper ballot" or "ballot" means the forms described in Article 8 of this chapter.

(32.1) "Scanning ballot" means a printed paper ballot designed to be marked by an elector with a ballot marking device or electronic ballot marker or a blank sheet of paper designed to be used in a ballot marking device or electronic ballot marker, which is then inserted for casting into a ballot scanner.

35) "Superintendent" means:

(A) Either the judge of the probate court of a county or the county board of elections, the county board of elections and registration, the joint city-county board of elections, or the joint city-county board of elections and registration, if a county has such;

(39) "Voter" is synonymous with the term "elector."

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA.gov Services Report

ICS Advisory (ICSA-22-154-01)

Vulnerabilities Affecting Dominion Voting Systems ImageCast X

Original release date: June 03, 2022

Legal Notice

---

1. SUMMARY

This advisory identifies vulnerabilities affecting versions of the Dominion Voting Systems Democracy Suite ImageCast X, which is an in-person voting system used to allow voters to mark their ballot. The ImageCast X can be configured to allow a voter to produce a paper record or to record votes electronically. While these vulnerabilities present risks that should be mitigated as soon as possible, CISA has no evidence that these vulnerabilities have been exploited in any elections.

Exploitation of these vulnerabilities would require physical access to individual ImageCast X devices, access to the Election Management System (EMS), or the ability to modify files before they are uploaded to ImageCast X devices. Jurisdictions can prevent and/or detect the exploitation of these vulnerabilities by diligently applying the mitigations recommended in this advisory, including technical, physical, and operational controls that limit unauthorized access or manipulation of voting systems. Many of these mitigations are already typically standard practice in jurisdictions where these devices are in use and can be enhanced to further guard against exploitation of these vulnerabilities.

2. TECHNICAL DETAILS

2.1 AFFECTED PRODUCTS

The following versions of the Dominion Voting Systems ImageCast X software are known to be affected (other versions were not able to be tested):

- ImageCast X firmware based on Android 5.1, as used in Dominion Democracy Suite Voting System Version 5.5-A

- ImageCast X application Versions 5.5.10.30 and 5.5.10.32, as used in Dominion Democracy Suite Voting System Version 5.5-A
    - **NOTE:** After following the vendor's procedure to upgrade the ImageCast X from Version 5.5.10.30 to 5.5.10.32, or after performing other Android administrative actions, the ImageCast X may be left in a configuration that could allow an attacker who can attach an external input device to escalate privileges and/or install malicious code. Instructions to check for and mitigate this condition are available from Dominion Voting Systems.

Any jurisdictions running ImageCast X are encouraged to contact Dominion Voting Systems to understand the vulnerability status of their specific implementation.

2.2 VULNERABILITY OVERVIEW

NOTE: Mitigations to reduce the risk of exploitation of these vulnerabilities can be found in Section 3 of this document.

2.2.1 IMPROPER VERIFICATION OF CRYPTOGRAPHIC SIGNATURE CWE-347

The tested version of ImageCast X does not validate application signatures to a trusted root certificate. Use of a trusted root certificate ensures software installed on a device is traceable to, or verifiable against, a cryptographic key provided by the manufacturer to detect tampering. An attacker could leverage this vulnerability to install malicious code, which could also be spread to other vulnerable ImageCast X devices via removable media.

CVE-2022-1739 has been assigned to this vulnerability.

2.2.2 MUTABLE ATTESTATION OR MEASUREMENT REPORTING DATA CWE-1283

The tested version of ImageCast X's on-screen application hash display feature, audit log export, and application export functionality rely on self-attestation mechanisms. An attacker could leverage this vulnerability to disguise malicious applications on a device.

CVE-2022-1740 has been assigned to this vulnerability.

2.2.3 HIDDEN FUNCTIONALITY CWE-912

The tested version of ImageCast X has a Terminal Emulator application which could be leveraged by an attacker to gain elevated privileges on a device and/or install malicious code.

CVE-2022-1741 has been assigned to this vulnerability.

2.2.4 IMPROPER PROTECTION OF ALTERNATE PATH CWE-424

The tested version of ImageCast X allows for rebooting into Android Safe Mode, which allows an attacker to directly access the operating system. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.

CVE-2022-1742 has been assigned to this vulnerability.

2.2.5 PATH TRAVERSAL: '../FILEDIR' CWE-24

The tested version of ImageCast X can be manipulated to cause arbitrary code execution by specially crafted election definition files. An attacker could leverage this vulnerability to spread malicious code to ImageCast X devices from the EMS.

CVE-2022-1743 has been assigned to this vulnerability.

2.2.6 EXECUTION WITH UNNECESSARY PRIVILEGES CWE-250

Applications on the tested version of ImageCast X can execute code with elevated privileges by exploiting a system level service. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.

CVE-2022-1744 has been assigned to this vulnerability.

2.2.7 AUTHENTICATION BYPASS BY SPOOFING CWE-290

The authentication mechanism used by technicians on the tested version of ImageCast X is susceptible to forgery. An attacker with physical access may use this to gain administrative privileges on a device and install malicious code or perform arbitrary administrative actions.

CVE-2022-1745 has been assigned to this vulnerability.

2.2.8 INCORRECT PRIVILEGE ASSIGNMENT CWE-266

The authentication mechanism used by poll workers to administer voting using the tested version of ImageCast X can expose cryptographic secrets used to protect election information. An attacker could leverage this vulnerability to gain access to sensitive information and perform privileged actions, potentially affecting other election equipment.

CVE-2022-1746 has been assigned to this vulnerability.

2.2.9 ORIGIN VALIDATION ERROR CWE-346

The authentication mechanism used by voters to activate a voting session on the tested version of ImageCast X is susceptible to forgery. An attacker could leverage this vulnerability to print an arbitrary number of ballots without authorization.

CVE-2022-1747 has been assigned to this vulnerability.

2.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS** Government Facilities / Election Infrastructure
- **COUNTRIES/AREAS DEPLOYED:** Multiple
- **COMPANY HEADQUARTERS LOCATION:** Denver, Colorado

2.4 RESEARCHER

J. Alex Halderman, University of Michigan, and Drew Springall, Auburn University, reported these vulnerabilities to CISA.

3. MITIGATIONS

CISA recommends election officials continue to take and further enhance defensive measures to reduce the risk of exploitation of these vulnerabilities. Specifically, for each election, election officials should:

- Contact Dominion Voting Systems to determine which software and/or firmware updates need to be applied. Dominion Voting Systems reports to CISA that the above vulnerabilities have been addressed in subsequent software versions.
- Ensure all affected devices are physically protected before, during, and after voting.
- Ensure compliance with chain of custody procedures throughout the election cycle.
- Ensure that ImageCast X and the Election Management System (EMS) are not connected to any external (i.e., Internet accessible) networks.
- Ensure carefully selected protective and detective physical security measures (for example, locks and tamper-evident seals) are implemented on all affected devices, including on connected devices such as printers and connecting cables.
- Close any background application windows on each ImageCast X device.
- Use read-only media to update software or install files onto ImageCast X devices.
- Use separate, unique passcodes for each poll worker card.
- Ensure all ImageCast X devices are subjected to rigorous pre- and post-election testing.
- Disable the “Unify Tabulator Security Keys” feature on the election management system and ensure new cryptographic keys are used for each election.
- As recommended by Dominion Voting Systems, use the supplemental method to validate hashes on applications, audit log exports, and application exports.
- Encourage voters to verify the human-readable votes on printout.
- **Conduct rigorous post-election tabulation audits of the human-readable portions of physical ballots and paper records, to include reviewing ballot chain of custody and conducting voter/ballot reconciliation procedures. These activities are especially crucial to detect attacks where the listed vulnerabilities are exploited such that a barcode is manipulated to be tabulated inconsistently with the human-readable portion of the paper ballot. (NOTE: If states and jurisdictions so choose, the ImageCast X provide the configuration option to produce ballots that do not print barcodes for tabulation.)**

Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov

Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics

or incident reporting: https://us-cert.cisa.gov/report