

April 11, 2023

Georgia State Election Board
2 MLK Jr. Drive
Suite 802 Floyd West Tower
Atlanta, GA 30334

Re: Petition for Amendment of Election Rules (Security Balloting, Audit, and Recount Rules)

Judge Duffey and Election Board Members:

Coalition for Good Governance respectfully submits the attached set of proposed amendments to the State Election Board Rules under the provisions Rule 183-1-1-.01. The purpose of the set of proposed amendments is to update Georgia's current Election Rules to reflect the security risks present in the state's electronic voting system, to address those risks through procedures to identify and respond to security threats, and establish specific steps for mitigation of certain risks.

Original notarized paper copies of the proposed amendments are being submitted to the State Election Board office as required by the above referenced Rule. We request that Board members review the electronic copies supplied by email in advance of the receipt of paper copies. We respectfully request that the proposed Rule amendments be heard and adopted at the next SEB meeting as required by Rule 183-1-1.01(4).

Requirements of Rule 183-1-1-.01(3)

(a) The name and post office address of the petitioner;

Coalition for Good Governance
P.O. Box 28097
Atlanta, GA 30358

Email:

Via email Marilyn@uscgg.org

Official corporate address:

Coalition for Good Governance
P.O. Box 754
Crestone, CO 81311

(b) The full text of the rule requested to be amended or repealed, or the full text of the rule desired to be promulgated;

Exhibits 1 – 6 attached.

(c) The reason(s) such rule should be amended, repealed, or promulgated;

The basis for the proposed rule amendments is stated as the introduction Exhibit 1. Further, the 2021 breach of the state's voting system software has not been mitigated, and poses an extreme cybersecurity risk to 2023 and 2024 elections. Such risks and the necessity of prompt

mitigation were explained by a group of cybersecurity and voting systems experts in the September 8, 2022 letter attached as Exhibit 7 and linked as well. (<https://coalitionforgoodgovernance.sharefile.com/d-s44dec3c27ada46c2ada04bb74b7e7924>) State and county officials took no action in response to the experts' recommendation, nor did the recently adjourned General Assembly. Our proposed amendments are intended to partially mitigate the escalated risks summarized by the experts.

Further, even prior to the known breach of the state's system, after reviewing Georgia's BMD system (Dominion ImageCastX), the U.S. Cybersecurity & Infrastructure Security Agency (CISA) issued an advisory concerning the touchscreen units stating that their "vulnerabilities present risks that should be mitigated as soon as possible." Additionally, CISA recommended as "especially crucial" rigorous post-election audits of all contests on the ballot. The report is attached as Exhibit 8 and also linked here. <https://www.cisa.gov/news-events/ics-advisories/icsa-22-154-01> State officials did not act on CISA's recommendations.

The risks presented by breach of Georgia's voting system are also summarized in a December 12, 2022 experts' letter to the Department of Justice and the Department of Homeland Security. No action has been taken by state or county officials to mitigate these serious and ongoing risks to fair and accurate elections.

<https://www.dropbox.com/s/jy3wxoxi605lyfs/DOJ.FBI.DHS.Coffee.GA.12.12.2022.pdf?dl=0>

In his February 24, 2022 deposition, in response to a question about risk to the voting system if "someone had imaged all the software in the voting system" and whether that would "create a risk to the voting system," Secretary of State representative Gabe Sterling testified "That would be a risk and vulnerability that we would probably have to *figure out some way to mitigate* if that was the case. We have no evidence that that's the case." (Curling Case Doc. 1368-5 p. 255) For at least a year, there has been clear publicly known irrefutable evidence of unauthorized imaging of the state's voting system equipment in Coffee County and numerous warnings of the extreme risk created. However, no meaningful mitigation measures have been undertaken. Mr. Sterling's acknowledgement of the need for mitigation is yet another clear reason that the rule amendments should be promptly adopted.

Additional reasons for amendment of the rules are also included in (d) below.

(d) Any and all pertinent existing facts as to the petitioner's interest in the matter;

The petitioner, Coalition for Good Governance, represents its Georgia-based members who are voters with very real interests in their rights to cast an accountable ballot in a secure system in exercising their constitutional right to vote. While it is infeasible to present "all pertinent existing facts as to the petitioner's interest in the matter," summaries of the concerns and interests are laid out in the Plaintiffs' recent responses to the Motion for Summary Judgment in the Curling v Raffensperger case. Pertinent documents containing hundreds of such existing facts are linked below:

Coalition Plaintiffs' Brief in Response to MSJ-

<https://coalitionforgoodgovernance.sharefile.com/d-s177adc95b2ec42b28edf416db28b5eb8>

Curling Plaintiffs' Brief in Response to MSJ -

<https://coalitionforgoodgovernance.sharefile.com/d-se211681936174051998d4d1c76e5d807>

Additional Statement of Facts—

<https://coalitionforgoodgovernance.sharefile.com/d-s2fda766de8d24dbca0d4965d278206af>

Plaintiffs' Response to Defendants' Statement of Facts -

<https://coalitionforgoodgovernance.sharefile.com/d-s770e8d4ded4e4db1a95985b2f0416a08>

Specifically, the highly escalated security risk to future elections after the statewide system breach initiated in Coffee County is detailed in expert reports from Kevin Skoglund and Professor J. Alex Halderman linked below:

Kevin Skoglund Report:

<https://coalitionforgoodgovernance.sharefile.com/d-sc17e2cde1fb54835b9ca9c73f7f8ea49>

J. Alex Halderman Report:

<https://coalitionforgoodgovernance.sharefile.com/d-s8f4bcb5f45d4453da6877a07224ad01e>

The requirement for more rigorous audits in the wake of the statewide security breach as recommended by CISA is supported in a report by **Professor Philip Stark:**

<https://coalitionforgoodgovernance.sharefile.com/d-sa08deaa0125340f48974d0669a1e5f76>

(e) Any and all facts known to the petitioner which might influence the decision of the Board to initiate or not initiate rulemaking, including identification of any parties who it is known will or may be affected by the amended, repealed, or promulgated rule; and

See above facts referenced in (c) and (d) above and the facts included in Exhibits 7 and 8 stating experts' and CISA's recommendations that immediate security mitigations be undertaken months ago. Neither the Secretary of State nor the State Election Board has acted to require or undertake such mitigations, and the November 2022 midterm elections were conducted with knowledge of risks of the system and the statewide breach and cybersecurity experts' recommendations that the security risks be addressed.

All Georgia voters and candidates likely benefit by adoption of a proposed rule securing the elections. Additionally, election officials at the municipal, county and state level will be required to undertake more security-oriented procedures which will affect their activities. The recommendations when implemented should substantially reduce the complexity and cost of conducting elections when hand marked paper ballots are used in compliance with the proposed rules.

Cities across the state are conducting important municipal elections in November 2023 and counties are preparing for presidential election year elections in 2024 using a compromised voting system, while the state is not addressing the extreme cybersecurity risks created by the 2021 breach. Urgent action such as adoption of recommended rules is required.

(f) Citations of legal authorities, if any, which authorize, support, or require the action requested by the petitioner.

The SEB's general authority for such rule-making is provided by O.C.G.A. § 21-2-31. Authority for use of emergency balloting by hand marked paper ballot is authorized by O.C.G.A. § 21-2-334. Authority for proposed recount and audit provisions is cited in the proposed rules in the exhibits. The requirement for the safety and accuracy of the ballot marking device system is required by O.C.G.A. § 21-2-379.24. See the federal court order detailing the risks of the BMD

system in the Curling v Raffensperger case for additional support for the action requested.
<https://coalitionforgoodgovernance.sharefile.com/d-sed61a0e7f9d5480f929c31027f1c80e3>

Additional information

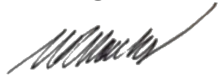
Certainly the limited use of touchscreen BMDs should continue for voters who wish to use them for accessibility needs. For such units, we recommend that the Secretary of State consider the use of Dominion's software application that marks a full face ballot with a non-uniform markings that resemble hand marked ballots to help protect ballot secrecy for voters who need to use the BMD units.

Our proposed amendments on Exhibits 1-6 are inserted in a copy of the applicable current complete rule. The proposed amended language is printed in red font and underlined.

We anticipate that other organizations and individuals may be joining us as informal co-petitioners in these proposed Rule amendments to partially address the serious unmitigated cybersecurity security risks to pending and future elections. We request that Coalition for Good Governance and potential co-petitioners be permitted to present the proposed amendments at the next SEB meeting consistent with practice of prior SEB hearings on such rule-making petitions.

Please contact me if we may provide more information that would be helpful to the Board.

Best regards,



Marilyn Marks
Executive Director
Coalition for Good Governance
Marilyn@uscgg.org
704 292 9802

(Notarized document included in original paper documents submitted.)

Verification of Petition for Amended Election Rules

I, Marilyn Marks, Executive Director of Coalition for Good Governance personally appeared before the undersigned public notary, duly authorized to administer oaths, and state under oath that every fact alleged in the Petition for Adoption of Rules dated April 11th, 2023 attached hereto is true and correct to the best of my knowledge, information and belief. I am duly authorized by Coalition for Good Governance to submit this petition on its behalf. The attached petition is submitted under the provisions of Rule 183-1-1-.01.

Dated this ___ day of April 2023.

Marilyn Marks

Sworn to and subscribed before me
This _____ day of April 2023.

Purpose of Security-Related Emergency Balloting, Audit and Recount Rules

The purpose of the Rules update is to ensure that SEB Rules provide proper guidance for county election officials to identify and respond to cybersecurity incidents and vulnerabilities to safeguard the state's critical voting system infrastructure and to maintain public confidence in the state's election processes. The Board recognizes the need for a standard set of mandatory procedures for rapid response for detection, communications, investigation, evaluation, containment, mitigation and remediation for cybersecurity vulnerabilities and incidents to drive coordinated state and county responsive actions, including inter-governmental responses. Accordingly, a continuing effort will be undertaken to consider appropriate response policies to inform a series of evolving mandatory rules that will be proposed for adoption over a number of months, and updated as technology changes, security considerations and governing law mandate.

Proposed rule changes recognize that a breach of the voting system occurred in 2021 in Coffee County and unauthorized individuals posted the contents of the election management system and scanners on online site, and such content has been shared with multiple other individuals. The Rule updates address the needed resulting mitigation well in advance of 2023 municipal elections and 2024 general elections and primaries.

183-1-12-.02 Definitions

(1) As used in this rule, the term:

- (a) "Ballot" shall have the meaning set forth in [O.C.G.A. § 21-2-2](#).
- (b) "Ballot scanner" shall have the meaning set forth in [O.C.G.A. § 21-2-2](#).
- (c) "Ballot Style" shall mean the specific offices, candidates, and questions displayed on an electronic ballot marker or paper ballot for voters according to their assigned precinct.
- (d) "Electronic ballot marker" shall have the meaning set forth in [O.C.G.A. § 21-2-2](#).
- (e) "Election management system" is an electronic system that contains databases for elections, allows for the creation of ballots, generates ballot scanner memory cards, and computes tabulated results, amongst performing other election functions.
- (f) "Electronic poll book" shall mean an electronic device that contains a list registered voters with sufficient information to look up voters, check them in, and encode voter access cards that bring up the correct ballot on an electronic ballot marker.
- (g) "Election Superintendent" or "superintendent" means a county board of elections and registrations, a county board of elections, a judge of the probate court, or an elections supervisor or director so designated by a county board or judge of the

probate court. For municipal elections, the term shall include the municipal counterparts set forth in [O.C.G.A. § 21-2-2](#).

(h) "Enclosed space" shall mean that area within a polling place enclosed with a guardrail or barrier closing the inner portion of such area so that only such persons as are inside such guardrail or barrier can approach within six feet of the ballot box, voting compartments, voting booths, voting machines, electronic ballot markers, or ballot scanners.

(i) "Opening of the Polls" shall mean the commencement of voting in a particular primary, election, or runoff. Opening of the polls does not refer to the unlocking or opening of the doors of the polling place. Similarly, the term "Closing of the Polls" shall mean the cessation of voting in a particular primary, election, or runoff and not the locking or closing of the doors of the polling place.

(j) "Poll officer" shall have the meaning set forth in [O.C.G.A. § 21-2-2](#).

(k) "Polling place" shall have the meaning set forth in [O.C.G.A. § 21-2-2](#).

(l) "Precinct" shall have the meaning set forth in [O.C.G.A. § 21-2-2](#).

(m) "Security incident" shall mean an occurrence that 1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, legal use, or availability of information of a voting system, or 2) constitutes a violation or imminent threat of violation of law, State Election Board Rule, security policies, security procedures, or acceptable use policies.

(n) "Security vulnerability" means any attribute of voting system hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(m-n) "Voter Access Card" shall mean the electronic card issued to a voter which is inserted into an electronic ballot marker to bring up the voter's correct ballot.

(n-o) "Zero Tape" shall mean a tape printed out by a ballot scanner unit which shows that no votes have been tabulated by the scanner for that election.

(e-p) "Voting system" or "voting system components" shall include electronic ballot markers, printers, ballot scanners, election management systems, electronic poll books, and voter access cards.

Statutory Authority

[O.C.G.A. §§ 21-2-2, 21-2-31](#).

History

Original Rule entitled "Vote Recorders" adopted. F. July 24, 1968; eff. August 12, 1968.

Repealed: New Rule entitled "Direct Recording Electronic Voting Equipment" adopted. F. Aug. 30, 2002; eff. Sept. 19, 2002. **Amended:** F. Oct. 24, 2003; eff. Nov. 13, 2003. **Amended:** F. May 11, 2004; eff. May 31, 2004. **Amended:** ER. 183-1-12-0.4-.02 adopted. F. Sept. 10, 2004; eff. Sept. 9, 2004, the date of adoption. **Amended:** F. Dec. 28, 2005; eff. Jan. 17, 2006.

Ga. Comp. R. & Regs. r. 183-1-12-.02

Repealed: New Rule of same title adopted. F. Oct. 29, 2009; eff. Nov. 18, 2009. **Repealed:** New Rule of same title adopted. F. Mar. 17, 2011; eff. Apr. 6, 2011. **Repealed:** New Rule entitled "Definitions" adopted. F. Jan. 23, 2020; eff. Feb. 12, 2020.

RULES AND REGULATIONS OF THE STATE OF GEORGIA
Copyright © 2023, Lawriter LLC All Rights Reserved.

End of Document

183-1-12-.05 Security of Voting System Components at County Elections Office or Designated County Storage Area

1. Software security. The software contained in electronic ballot markers, ballot scanners, election managements systems, and electronic poll books, regardless of whether the unit is owned by the county or the State, shall not be modified, upgraded, or changed in any way without the specific prior approval of the Secretary of State.
2. Electronic ballot markers, ballot scanners, and election management systems shall not be connected to the internet and no other software shall be loaded onto or maintained or used on computers on which the election management system software is located except as specifically authorized by the Secretary of State.
3. The room in which the election management system is located shall be locked at all times when the system is not directly under the supervision of the election superintendent or his or her designee. Lock and key access to the room where the election management system is located shall be limited to the county election superintendent; the election supervisor, if any; personnel of the county election superintendent's office designated by the county election superintendent; building maintenance personnel; and emergency personnel. Building maintenance personnel shall have access to the room in which the election management system is located only to the extent necessary to carry out their maintenance duties. The election superintendent shall maintain on file at all times in the office of the election superintendent a complete and up to date list of all maintenance personnel with access to the room in which the election management system is located. Emergency personnel shall have access to the room in which the election management system is located only as necessary in the event of an emergency and only for the duration of such emergency condition.
4. The election management system shall remain password-locked at all times when not in use.
5. While in storage at the county elections office or designated county facility, all components of the voting system (including electronic ballot markers, ballot scanners, electronic poll books, ballot boxes, and election management systems) shall be stored under lock and key at all times when not in use. Lock and key access to such items shall be limited to the county election superintendent; members of the county board of elections; the election supervisor, if any; personnel of the county election superintendent's office designated by the county election superintendent; building maintenance personnel; and emergency personnel. Building maintenance personnel shall have access to the area where such items are stored only to the extent necessary to carry out their maintenance duties. The election superintendent shall maintain on file at all times in the office of the election superintendent a complete and up to date list of all maintenance personnel with access to the area in which such items are stored. Emergency personnel shall have access to the area where such items are stored only as

necessary in the event of an emergency and only for the duration of such emergency condition. Whenever maintenance or emergency personnel are required to enter the storage area, the election superintendent must be notified of that entry as soon as possible and the election superintendent must maintain a log of those persons who entered the storage area.

6. Security Incidents and Vulnerabilities. County and municipal election superintendents shall immediately submit a written statement reporting all suspected security incidents, regardless of severity, in the fullest detail possible including photographs and video recordings if feasible, to the Secretary of State and the State Election Board. The State Election Board shall promptly undertake an investigation of the scope of the reported suspected incident and alert other appropriate officials, including law enforcement authorities.

- (a) County and municipal election superintendents shall collect, safeguard, and preserve all data related in any manner to the incident, including but not limited to video surveillance security recordings, scanner memory cards, the EMS server, activity logs, election databases including ballot images, paper ballots, and all manual and electronic records relating to elections within 6 months of the suspected incident. Such records shall be preserved until written permission of the State Election Board and the Secretary of State is obtained.
- (b) Election superintendents shall fully comply with incident response reporting, record preservation, and mitigation requirements as detailed in the Secretary of State's incident response policy.
- (c) Election superintendents shall promptly submit a written report to the Secretary of State and the State Election Board all voting system security vulnerabilities which come to their attention. The report shall be in writing with the fullest possible detail, including photographs and video records if feasible, and be submitted no later than 24 hours after such vulnerability is detected.

Statutory Authority

[O.C.G.A. § 21-2-31.](#)

History

Original Rule entitled "Ballot Envelopes" adopted. F. July 24, 1968; eff. August 12, 1968.

Amended: F. Aug. 5, 1969; eff. Aug. 24, 1969. **Repealed:** New Rule entitled "Ballot Envelopes and Fold Over Ballot Cards" adopted. F. May 26, 1970; eff. June 14, 1970. **Amended:** F. Mar. 6, 1987; eff. Mar. 26, 1987. **Repealed:** F. Dec. 11, 2003; eff. Dec. 31, 2003. **Adopted:** New Rule entitled "Security of Voting System Components at County Elections Office or Designated County Storage Area." F. Jan. 23, 2020; eff. Feb. 12, 2020.

183-1-12-.01 Conduct of Elections

Beginning with the 2020 Presidential Preference Primary, all federal, state, and county general primaries and elections, special primaries and elections, and referendums in the State of Georgia shall be conducted via an Optical Scanning Voting System as defined by [O.C.G.A. 21-2-1\(19.1\)](#). Voting at the polls, including both Election Day and absentee-in-person voting shall be conducted via ballots marked by electronic ballot markers and tabulated by ballot scanners. The electronic ballot markers and ballot scanners shall be supplied by the Secretary of State or purchased by the counties with the authorization of the Secretary of State. Absentee-by-mail voting shall also be conducted through the use of an optical scanning voting system.

The Superintendent shall cause every polling place and advance voting location to have a sufficient number of blank paper ballots that can be marked by pen available for use in the event of emergency. The election superintendent shall also be prepared to resupply polling places with emergency paper ballots in needed ballot styles in a timely manner while voting is occurring so that polling places do not run out of emergency paper ballots.

- (a) In the event of an identified security incident involving the state's or a county's voting system, the election superintendent's use of emergency balloting as provided in Rule 183-1-12-.11(2)(c and d) is authorized and recommended as an appropriate immediate response until such time as the detected incident is evaluated by security professionals, and mitigation and remediation procedures, if necessary, are approved for implementation by the State Election Board and the Secretary of State.
- (b) If the contents of an EMS server or hard drive of ballot scanners or a copy of the voting system software are reasonably believed to have been accessed or obtained by unauthorized persons, emergency balloting procedures as provided in Rule 183-1-12-.11-1(c, d) and supplemental post-audits as provided in Rule 183-1-15-.04 (3) shall be used following the conduct all elections, primaries and runoff elections until such time as the electronic ballot marking device voting system is declared safe for use by the Secretary of State and a majority vote of the State Election Board, following a public hearing.

Statutory Authority

[O.C.G.A. §§ 21-2-1, 21-2-31.](#)

History

Original Rule entitled "Voting Machines" adopted. F. July 24, 1968; eff. August 12, 1968.

Repealed: New Rule entitled "Conduct of Elections" adopted. F. Aug. 30, 2002; eff. Sept. 19, 2002. **Amended:** F. Oct. 24, 2003; eff. Nov. 13, 2003. **Repealed:** New Rule of same title adopted. F. Jan. 23, 2020; eff. Feb. 12, 2020.

Ga. Comp. R. & Regs. r. 183-1-12-.01

RULES AND REGULATIONS OF THE STATE OF GEORGIA
Copyright © 2023, Lawriter LLC All Rights Reserved.

End of Document

183-1-12-.11 Conducting Elections

1. As each voter presents himself or herself at the polling place for the purpose of voting during the time during which the polls are open for voting, each voter shall be offered instruction by a poll officer in the method of voting on the voting system. In providing such instruction, the poll officers shall not in any manner request, suggest, or seek to persuade or induce any voter to vote any particular candidate, political party, or political body, or for or against any particular question.

2.

(a) When a person presents himself or herself at the polling place for the purpose of voting during the time during which the polls are open for voting, the person shall complete a voter certificate and submit it to the poll officers. The voter certificate may be an electronic or paper record. The poll officers shall verify the identity of the person and that the person is a registered voter of the precinct and, if so, shall approve the voter certificate and enter an appropriate designation on the electors list for the precinct reflecting that the voter has voted in the primary, election, or runoff being conducted. The voter's name shall then be entered on the appropriate numbered list of voters.

(b) A poll officer shall then issue the voter an appropriate voter access card authorizing the voter to vote the correct ballot on the touchscreen or utilize the correct access code to manually bring up the correct ballot on the touchscreen. The voter shall then enter the enclosed space in the polling place and proceed to vote his or her choices. Upon making his or her selections, the voter shall cause the paper ballot to print, remove his or her printed ballot from the printer, remove the voter access card from the touchscreen component, review the selections on his or her printed ballot, scan his or her printed ballot into the scanner, and return the voter access card to a poll officer. Then the voter shall exit the enclosed area of the polling place.

(c) If an emergency situation makes utilizing the electronic ballot markers impossible or impracticable, as determined by the election superintendent, Secretary of State, or the State Election Board, the poll officer shall issue the voter an emergency paper ballot that is to be filled out with a pen after verifying the identity of the voter and that the person is a registered voter of the precinct. Emergency paper ballots shall not be treated as provisional ballots, but instead shall be placed into the scanner in the same manner that printed ballots in the polling place are scanned. The election superintendent shall cause each polling place to have a sufficient amount of emergency paper ballots so that voting may continue uninterrupted if emergency circumstances render the electronic ballot markers or printers unusable. For any primary or general election for which a state or federal candidate is on the ballot, a sufficient amount of emergency paper ballots shall be at least 10% of the number of registered voters to a polling place. The poll manager shall store all emergency ballots in a secure manner and ensure that all used and unused emergency ballots are

accounted for. All unused emergency ballots shall be placed into a secure envelope and sealed such that the envelope cannot be opened without breaking such seal.

(d) If an emergency situation exists that makes voting on the electronic ballot markers impossible or impracticable, the poll manager shall alert the election superintendent as soon as possible. The existence of an emergency situation shall be in the discretion of the election supervisor. However, if a poll manager is unable to contact the election superintendent after diligent effort, the poll manager shall have the ability to declare that an emergency situation exists at the polling place. The poll manager shall continue diligent efforts to contact the election superintendent, and shall inform the superintendent as soon as possible of the situation at the polling place. The election superintendent, in his or her discretion, shall either overrule or concur with the declaration of emergency circumstances. While the determination of an emergency situation is in the discretion of the election superintendent, the types of events that may be considered emergencies are power outages, malfunctions causing a sufficient number of electronic ballot markers to be unavailable for use, or waiting times longer than 30 minutes.

3. At least once each hour during the time while the polls are open, the poll officers shall examine the enclosed space to verify that no unauthorized matter has been affixed to any voting system component or placed in the voting booth and that the voting system components have not been tampered with in any manner. Poll officers shall also check that no unattended ballots are left in the printer or anywhere in the enclosed space other than the appropriate ballot box. Any unattended ballots found in the enclosed space that do not belong to a voter currently in the enclosed space shall not be counted, but shall be secured and labelled as unattended ballots.

4. The polling place shall be arranged in such a manner as to provide for the privacy of the elector while voting and to allow monitoring of each voting system component by the poll officers while the polls are open. The electronic ballot markers and ballot scanners used in the polling place shall be set up in a manner to assure the privacy of the elector while casting his or her ballot while maintaining the security of such units against tampering, damage, or other improper conduct. In addition, at least one ballot marking device shall be configured for voting by physically disabled voters in wheelchairs and provisions shall be made to provide for the privacy of such electors while voting.

5. It shall be permissible under [O.C.G.A. § 21-2-410](#) and shall not constitute assistance in voting under [O.C.G.A. § 21-2-409](#) for poll officers to assist a voter in inserting the voter access card into the ballot marking device and in explaining the operation of the unit to the voter; provided that the poll officer shall withdraw from the voting booth prior to the voter making any selections. The poll officers shall not in any manner request, suggest, or seek to persuade or induce any voter to vote for any particular candidate, political party, or political body, or for or against any particular question.

6. Voters utilizing an audio tactile interface (ATI) device to vote on the ballot marking device without the assistance of any other individual shall not be considered as receiving assistance in voting and shall not be required to complete the forms required for receiving assistance in voting pursuant to [O.C.G.A. § 21-2-409](#); however, if another person other

than a poll officer is handling the printed ballot before it is inserted into the scanner, that person shall be considered as assisting.

7. The poll officers shall confirm that voters deposit their ballots and return the voter access cards to the poll officers prior to leaving the enclosed space in the polling place. The poll officers shall arrange and configure the polling place and provide staffing at such places within the polling place to confirm that a voter will not leave the enclosed space with a ballot or voter access card.

8. The election superintendent shall cause each polling place to be sufficiently staffed. At least one poll officer shall be assigned to assisting voters who have questions while they are in the voting booth but before they approach the ballot scanner. Another poll officer shall be stationed at every ballot scanner in use in the polling place while voting is occurring. The poll officer stationed at the ballot scanner shall offer each voter specific verbal instruction to review their printed paper ballot prior to scanning it. In addition to the preceding instruction, the poll officer stationed at the ballot scanner shall offer general instruction throughout the period while voting is occurring telling voters that sample ballots and magnifying devices are available to assist them in reviewing their paper ballot. The poll officer shall take all reasonable precautions not to view the selections on an elector's ballot unless it is required due to assistance requested by the elector. If a poll officer observes a voter attempting to leave the enclosed space with a paper ballot, the poll officer shall inform the voter of the consequence of not depositing his or her paper ballot into the ballot scanner prior to leaving the room.

9. A voter may request information from poll officers concerning how to use the electronic ballot marker or any other voting system component at any time during the voting process. However, once the voter scans his or her ballot into the ballot scanner, even if the ballot is blank with no votes cast, such voter shall be deemed to have voted and may not thereafter vote again. If a voter leaves the room encompassing the enclosed space with his or her paper ballot and does not place that ballot into the appropriate ballot scanner or ballot box, that voter shall be deemed to have voted and may not thereafter vote again. A sign shall be placed at the exit of the enclosed space that informs every voter that ballots may not be removed from the enclosed space. Any paper ballot that is removed from the room encompassing the enclosed space shall not be counted and shall be marked as spoiled by a poll officer.

10.

(a) If a voter discovers that the ballot presented on the electronic ballot marker is not correct or, for a partisan primary, is not the ballot that the voter desired to vote, the voter shall immediately notify a poll officer. The poll officer shall cancel or void the ballot on the electronic ballot marker without attempting in any manner to see how the voter has voted and shall then take the necessary steps to provide the voter with the correct ballot and make any necessary corrections to the voter certificate of the voter, the electors list, and the numbered list of voters. If the error is due to equipment malfunction, the poll officer shall document the incident on a form developed by the Secretary of State. The poll manager shall inform the election superintendent immediately if one or more electronic ballot markers are associated with a significant number of incidents.

(b) If, while reviewing his or her printed ballot, the voter discovers that the printed ballot does not contain the proper ballot selections or that the voter was not issued the proper ballot, the voter shall immediately inform a poll officer. The poll officer shall spoil the paper ballot and take the necessary steps to allow the voter to make his or her selections again on the electronic ballot marker and cause the correct ballot to be issued. If the error is due to equipment malfunction, the poll officer shall document the incident on a form developed by the Secretary of State. The poll manager shall inform the election superintendent immediately if one or more electronic ballot markers are associated with a significant number of incidents.

(c) If the voter places his or her paper ballot into the ballot scanner or ballot box prior to notifying the poll officials of any errors in the ballot, the voter shall be deemed to have voted and shall not be permitted to cast another ballot.

11.

(a) If any voting system component malfunctions during the day of a primary, election, or runoff, the poll manager shall immediately notify the election superintendent and shall not allow any voter to use the component until and unless the malfunction is corrected. The poll manager shall utilize appropriate backup procedures so that voting is not interrupted due to any equipment malfunctions. The election superintendent shall immediately arrange for the repair of the voting system component or shall provide a replacement component as soon as practicable. A replacement component shall not be used unless it has been appropriately tested prior to its use.

(b) In the event that a ballot scanner malfunctions, the voter shall place their voted ballot in the emergency bin connected to the ballot box. The ballots in the emergency bin shall be counted when the ballot scanner is properly functioning, by a replacement ballot scanner brought to the polling place, or, if neither are available, by another scanner at the county elections office. Poll officers may scan ballots placed into the emergency bin through the ballot scanner or a replacement ballot scanner when doing so will not interfere with voting. A voter placing his or her ballot into the emergency bin is considered to have voted that ballot and shall not be permitted to cast another ballot.

(c) Accredited poll watchers shall be allowed to observe the process described in this rule; however, they must do so in a manner that does not interfere with poll officials or voters.

12. Polling Place Wait Time Recordings

(a) On the day of any state or federal general primary, election, or runoff therefrom, the chief manager of a precinct shall measure and record the time a voter waits in line prior to checking into vote.

(b) The wait times shall be measured a minimum of three times while voting is occurring, in accordance with the following specifications:

- i. Morning wait times shall be measured only during the hours between 7:00AM and 11:00AM.

Ga. Comp. R. & Regs. r. 183-1-12-.11

ii. Midday wait times shall be measured only during the hours between 11:00AM and 3:00PM.

iii. Evening wait times shall be measured only during the hours of 3:00pm and 7:00PM.

(c) Such results shall be recorded on a form provided by the Secretary of State and provided electronically in a manner determined by the Secretary of State.

Statutory Authority

[O.C.G.A. §§ 21-2-31, 21-2-263, 21-2-409, 21-2-410.](#)

History

Original Rule entitled "Conducting Elections" adopted. F. Jan. 23, 2020; eff. Feb. 12, 2020.

Amended: F. Mar. 2, 2020; eff. Mar. 22, 2020. **Amended:** F. Sep. 22, 2021; eff. Oct. 12, 2021.

RULES AND REGULATIONS OF THE STATE OF GEORGIA

Copyright © 2023, Lawriter LLC All Rights Reserved.

End of Document

183-1-15-.03 Recount Procedure

(1) Recount by Electronic Tabulation

- (a) Recounts of primaries and elections conducted using an optical scanning voting system shall be in accordance with this rule.
- (b) The recount shall be conducted by tabulating all ballots utilizing ballot scanners.
- (c) Prior to conducting a recount, the election superintendent shall test each ballot scanner to be used in the recount. A test deck shall be prepared to include at least 75 ballots marked by an electronic ballot marker and 25 absentee ballots marked by hand that were cast in the election to be recounted. The ballots shall be selected from at least 3 different precincts, if available. The selection of individual ballots from a precinct's ballot container shall be conducted in a manner that selects ballots from throughout the ballot container. The test deck shall be tabulated by the ballot scanner or scanners to be used in the recount using one or more batches. A manual hand count of the test deck shall be made and compared to the electronic tabulation of the test deck. If the two counts do not match, the discrepancy shall be researched and additional tests may be run. If the discrepancy cannot be resolved so that the manual hand count and electronic tabulation of the test deck matches, the ballot scanner shall not be used in the recount. If, after testing all available ballot scanners, there are no ballot scanners authorized to be used in the recount, the recount shall be conducted by manual hand count. Upon completion of the test, the test deck ballots shall be returned to their original ballot containers.
- (d) The recount shall be open to the view of the public, but no person except one designated by the superintendent or the superintendent's authorized deputy shall touch any ballot or ballot container. The superintendent may designate a viewing area by which members of the public are limited for the purpose of good order and maintaining the integrity of the recount.
- (e) The tabulation of ballots must be completed through a precise, controlled process that ensures, for each ballot scanner used in the recount, no more than one ballot container is unsealed at any given time.
- (f) A clear audit trail must be maintained at all times during the recount, including but not limited to, a log of the seal numbers on ballot containers before and after the recount.
- (g) The ballot scanner shall be programmed to flag or reject ballots that contain an overvote for the contest to be recounted. One or more recount vote review panels shall be established, consistent with [O.C.G.A. § 21-2-483\(g\)](#), to manually review the overvoted ballots. The recount vote review panel shall determine by majority vote the elector's intent, as described in [O.C.G.A. § 21-2-438\(c\)](#), a duplicate ballot shall be created consistent with the elector's intent for the contest to be recounted, labeled

"RECOUNT DUPLICATE", and used in the recount. The original overvoted ballot shall be retained.

(h) All ballots that required a duplicate ballot to be created in the original primary or election, as allowed by law, shall be reviewed by a recount vote review panel to determine that the votes marked in the contest to be recounted on the duplicated ballot are consistent with the elector's intent on the original ballot, as described in [O.C.G.A. § 21-2-438\(c\)](#). If a majority of the recount vote review panel determine that the duplicated ballot is not consistent with the elector's intent on the original ballot, a new true duplicate ballot shall be created consistent with the elector's intent for the contest to be recounted, labeled "RECOUNT DUPLICATE", and used in the recount. The original overvoted ballot and initial duplicated ballot shall be retained.

(i) If it appears that a ballot is so torn, bent, or otherwise defective that it cannot be processed by the ballot scanner, the recount vote review panel shall prepare a duplicate ballot for the contest to be recounted. All duplicate ballots created during the recount shall be clearly labeled by the word "RECOUNT DUPLICATE". The defective ballot shall be retained.

(j) After all of the valid ballots to be included in the recount have been tabulated, the superintendent shall cause a printout to be made of the results and shall compare the results to the results previously obtained. If upon completing the recount, it shall appear that the original vote count for the recounted contest was incorrect, such returns and all papers being prepared by the superintendent shall be corrected accordingly.

(2) Recount by Manual Hand Count

(a) A recount shall be conducted by manual hand count only:

1. As provided under [Rule 183-1-15-.03\(1\)\(c\)](#); or
2. [As provided under \[proposed\] Rule 183-1-15-04-\(3\)\(1\); or](#)
3. [At the discretion of the Secretary of State for state or federal office elections and the election superintendent for elections for other offices or ballot questions; or](#)
- ~~3~~ 4. Pursuant to a court order.

(b) Votes shall be counted by one or more recount teams consisting of at least three persons each. The superintendent shall select the persons for each recount team.

(c) In a recount of a partisan election, the recount team shall be composed of the election superintendent or designee thereof and one person selected by the election superintendent from a list provided by the county executive committee of each political party and body having candidates whose names appear on the ballot for such election, provided that, if there is no organized county executive committee for a political party or body, the person shall be selected from a list provided by the state executive committee of the political party or body. If, after the superintendent provides reasonable notice and a deadline to the executive committee, a county executive committee or state executive committee does not provide a sufficient number of names or does not timely delivery the list of names, the superintendent shall be

permitted to select the persons to serve on the recount team on behalf of the political party or body as needed.

(d) In a recount of a nonpartisan election, the recount team shall be composed of the election superintendent or designee thereof and two electors of the county, in the case of a county election, or the municipality, in the case of a municipal election, selected from a list provided by the chief judge of the superior court of the county in which the election is held or, in the case of a municipality which is located in more than one county, of the county in which the city hall of the municipality is located. If, after the superintendent provides reasonable notice and a deadline to the chief judge, the chief judge fails to designate a sufficient number of persons for the recount or does not timely delivery the list of names, the superintendent shall be permitted to select the persons to serve on the recount team as needed.

(e) Ballots shall be manually counted by hand in batches of no more than 30 to ensure that the number of ballots recounted matches the number originally counted.

(f) The recount teams shall determine the elector's intended vote on each ballot, by majority vote, in accordance with [Rule 183-1-15-.02](#). In the event of a tie vote by a review team, the vote of the election superintendent or designee thereof shall control.

(g) Recount teams shall compare the number of votes, overvotes, and undervotes to the number of ballots in the batch. If the numbers do not match, the batch shall be counted again.

(h) After all of the valid ballots to be included in the recount have been counted, the superintendent shall compare the results of the recount to the results previously obtained. If upon completing the recount, it shall appear that the original vote count for the recounted contest was incorrect, such returns and all papers being prepared by the superintendent shall be corrected accordingly.

Statutory Authority

[O.C.G.A. §§ 21-2-31, 21-2-495.](#)

History

Original Rule entitled "Optical Scan Recount Procedure" adopted. F. Mar. 2, 2020; eff. Mar. 22, 2020. **Amended:** New title "Recount Procedure." F. May 8, 2020; eff. May 28, 2020.

183-1-15-.04 Audit

(1) Preparing for the Audit

1. Following November general elections in even-numbered years, each county shall participate in a statewide risk-limiting audit with a risk limit of not greater than 10 percent as set forth in this rule prior to the certification by the Secretary of State.
2. Prior to county certification, the election superintendent of each county shall prepare a ballot manifest as instructed by the Secretary of State.
3. The contest to audit shall be selected by the Secretary of State. The Secretary of State shall set a date, time, and location after the November general election in even-numbered years to select which contest to audit. Such meeting shall be open to the public. After selecting the contest to audit, the Secretary of State shall publicly announce which contest will be audited and publish the selected contest on the Secretary of State webpage. In selecting the contest to audit, the Secretary of State shall consider the below criteria:
 - a. The closeness of the reported tabulation outcomes;
 - b. The geographical scope of the contests;
 - c. The number of ballots counted in the contests;
 - d. Any cause for concern regarding the accuracy of the reported tabulation outcome of the contests;
 - e. Any other benefits that may result from auditing certain contests; or
 - f. The ability of the county to complete the audit before the state certification deadline.
4. The audit shall be open to the public, and public notice of the date, time, and location of the audit must be posted on the county election office's website, or, if the county election's office does not have a website, in another prominent location.

(2) Conducting the Audit

1. The audit shall be open to the view of the public and press, but no person except the person(s) designated by the election superintendent or the superintendent's authorized deputy shall touch any ballot or ballot container. The election superintendent may designate a viewing area from which members of the public may observe the audit for the purpose of good order and maintaining the integrity of the audit.
2. The election superintendent shall create audit teams comprised of at least two sworn designees to assist with the audit. The superintendent may designate non-employees to assist with the audit process. All persons who the superintendent

designates to assist with the audit shall take and sign an oath that they will conduct the audit accurately and securely prior to assisting with the audit.

3. Chain of custody for each ballot shall be maintained at all times during the audit, including but not limited to, a log of the seal numbers on the ballot containers before and after completing the manual audit.
4. For ballots marked by electronic ballot markers, the auditors shall rely on the printed text on the ballot to determine the voter's selection. For ballots marked by hand, the auditors shall rely on the choices indicated by the voter by filling in the oval adjacent to the candidate or question.
5. The audit shall end once all selected ballots have been counted and the risk limit for the audit has been met.
6. The election superintendent shall report the results of the audit to the Secretary of State.
7. The election superintendent shall follow instructions issued by the Secretary of State on how to specifically conduct the audit, including but not limited to setting deadlines and formats for creating ballot manifests.

(3) Supplemental Audits

Supplemental post-election audits shall be conducted by the superintendent at the direction of the Secretary of State, for all county, state, and federal elections, primary elections and runoffs conducted after a security incident has been reported to the State Election Board and prior to a final determination by the State Election Board and the Secretary of State that the voting system is secure for use. No less than 50% of the contested election races on the ballot shall be audited using Risk Limiting Audit procedures as specified by the Secretary of State, or a full hand count audit at the discretion of the superintendent. The goal of the audit is to ensure that the correct winner is declared, without requiring confirmation of the exact tallies reported. The contested races selected for auditing at least 50% of such races shall be determined by random selection, but may be supplemented at the discretion of the superintendent.

1. If material discrepancies are detected in the post-election audit, a full manual recount shall be conducted under the provisions of Rule 183-1-15.03(2).
2. No supplemental audit shall be required if a full discretionary manual recount is conducted under the provisions of O.C.G.A. §21-2-495(a) or (d) and Rule 183-1-15.03(2). A candidate's or political party's request for such discretionary recount shall be heard and decided by the election superintendent in a publicly noticed meeting.

Statutory Authority

[O.C.G.A. §§ 21-2-31, 21-2-498.](#)

History

Original Rule entitled "Audit" adopted. F. Sep. 24, 2020; eff. Oct. 14, 2020.

Ga. Comp. R. & Regs. r. 183-1-15-.04

RULES AND REGULATIONS OF THE STATE OF GEORGIA
Copyright © 2023, Lawriter LLC All Rights Reserved.

End of Document

September 8, 2022

Georgia State Elections Board
Mr. William S. Duffey, Jr., Chair
Mr. Matthew Mashburn, Member
Mrs. Sara Tindall Ghazal, Member
Mr. Edward Lindsey, Member
Dr. Janice W. Johnston, Member
Secretary of State Brad Raffensperger, Ex Officio
214 State Capitol
Atlanta, Georgia 30334

Dear Chair Duffey and Members of the State Elections Board:

Media reports have recently confirmed allegations that Georgia’s voting system software was accessed and copied by several unauthorized individuals. These individuals handled the sensitive files in a reckless manner, transferring them to numerous people over the internet, who also have no authority to possess the state’s voting software and data.¹

As members of the computer science, cybersecurity, and election integrity communities,² we are writing to provide important context regarding the serious threats this security breach poses to Georgia’s elections, and to urge you to address the issue by taking specific actions to mitigate the heightened risks.

The immediate concern

The Secretary of State claims that his office has adequately addressed this security breach by replacing one server in the one currently known affected county. Replacing the server does not mitigate the breach, for reasons we shall explain.

The illegal copying of software and data (“disk images”) from the Georgia election management system (EMS) and voting device software, which occurred more than

¹ Emma Brown, Jon Swaine, Aaron C. Davis, Amy Gardner, “Trump-allied lawyers pursued voting machine data in multiple states, records reveal,” *The Washington Post*, August 15, 2022. Available at: <https://www.washingtonpost.com/investigations/2022/08/15/sidney-powell-coffee-county-sullivan-strickler/>

² The undersigned are all experts in election cybersecurity. Each of us has well over a decade of continuous experience in that field and a long history of conducting technical studies of voting systems or voting system-related cybersecurity, as well as writing, speaking, testifying, making media appearances on many aspects of election integrity.

20 months ago, constitutes a serious threat to Georgia’s election security. Those images, which include the EMS, and its installation environment, were accessed improperly by individuals and entities that have engaged in a campaign aimed at overturning the 2020 election results in Georgia and other key states.³ While it is prudent to assume that other nation states have had that software for a long time, now countless individuals with unknown affiliations, motives, and physical access to voting systems have it also. This increases both the risk of undetected cyber-attacks on Georgia, and the risk of accusations of fraud and election manipulation. Without trustworthy, physical records of voter intent (recorded by the hand of the voter, not with vulnerable, computerized ballot marking devices), rigorous chain of custody of ballots, and rigorous post-election auditing, such allegations will be difficult, if not impossible, to disprove.

Georgia’s elections have a higher risk of compromise due to the reliance on computerized Ballot-Marking Devices (BMDs) to record vote selections for in-person voting.

To ensure resiliency, auditability and transparency in an election, it is essential that there be a reliable, trustworthy record of each voter’s selections; this provides ground truth of voter intent.⁴ This record should be the record used for audits and recounts. Having a trustworthy physical record of voter intent allows administrators to check and confirm that the vote tabulation is correct, and to catch and correct any errors that may have occurred—regardless of their source.

In 2020 Georgia finally abandoned its insecure, paperless, touchscreen Diebold voting machines. Ignoring recommendations from election security experts⁵ and public preference,⁶ the Secretary of State successfully pushed the State legislature to approve a universal use BMD touchscreen voting system. The BMD system has put Georgia’s elections at a higher risk for tampering, disruption, or allegations of

³ Tierney Sneed, “Judge sanctions pro-Trump lawyers who brought ‘frivolous’ lawsuits,” *CNN*, August 26, 2022. Available at: <https://www.cnn.com/2021/08/25/politics/judge-sanctions-powell-wood-kraken-lawsuits/index.html>

⁴ “Report of the Auditability Working Group,” National Institute of Standards and Technology, 2010. Available at: <https://www.nist.gov/document/auditabilityreportxml-7htm>

⁵ Dr. Wenke Lee, the only computer security expert on Secretary Raffesperger’s “Secure, Accessible, Fair, Elections (SAFE) Commission, vigorously opposed the universal use of ballot marking devices. Dr. Lee’s position was supported by 24 computer security experts who urged the SAFE Commission to recommend against the universal use of BMDs.

⁶ Mark Neisse, “AJC poll: Georgians support paper ballots and oppose voter purges,” *Atlanta Journal Constitution*, January 21, 2019. Available at: <https://www.ajc.com/news/state--regional-govt--politics/ajc-poll-georgians-support-paper-ballots-and-oppose-voter-purges/mkdeIgUXtzJL6TFVbM6BVP/>

manipulation because all votes cast in a polling location are recorded using vulnerable, computerized BMDs, and tabulated from QR codes, which voters cannot check. The software breach in Coffee County has further increased this risk.

Vulnerabilities in the Ballot Marking Device (BMD) software can be exploited to mis-record votes.

While serving as an expert witness in the *Curling v. Raffensperger* lawsuit in federal court in Georgia, University of Michigan computer science professor J. Alex Halderman, one of the nation's foremost experts in voting system cybersecurity, analyzed Dominion ICX BMD (touchscreen and printer) software. Dr. Halderman found serious security vulnerabilities, some of which would allow a voter to infect a BMD with malware while voting, with little likelihood of detection. That malware could make the BMD print incorrect votes and spread silently to other voting machines and the central election management system in the county. Halderman's findings confirm that Dominion ICX BMD printout is not a reliable record of voter intent.⁷

The judge in *Curling* considered Prof. Halderman's full report, dated July 1, 2021, so sensitive that she ordered the report to be sealed. Halderman's follow-on report, dated July 13, 2021, is public and summarizes some of the conclusions of this sealed report.⁸ Prof. Halderman's findings were so concerning that he presented them to the Department of Homeland Security's Cybersecurity and Infrastructure

⁷ Research shows that voters rarely check machine-printed votes and rarely notice errors when they do check. No audit can determine whether ballot-marking devices printed voters' true selections: if a substantial number of voters use ballot-marking devices, no audit can limit the risk that an incorrect electoral result will be certified. See, e.g., Appel, A., R.A. DeMillo, and P.B. Stark, 2020. Ballot-Marking Devices Cannot Ensure the Will of the Voters, *Election Law Journal: Rules, Politics, and Policy*, 19, <https://doi.org/10.1089/elj.2019.0619>; Seventh Declaration of Philip B. Stark, 13 September 2020. *Curling et al. v Raffensperger et al.*, United States District Court for the District of Georgia, Northern Division 1:17-cv-2989-AT <https://coalitionforgoodgovernance.sharefile.com/share/view/s5ae19303763c45dfa5c8238cb58e47d8> (last visited 2 September 2021); Eighth Declaration of Philip B. Stark, 2 August 2021. *Curling et al. v Raffensperger et al.*, United States District Court for the District of Georgia, Northern Division 1:17-cv-2989-AT <https://coalitionforgoodgovernance.sharefile.com/share/view/sbda3c49bc6b646579d6691fb68f2d840> (last visited 2 September 2021)

⁸ Declaration of J. Alex Halderman, 2 August 2021. *Curling et al. v Raffensperger et al.*, United States District Court for the District of Georgia, Northern Division 1:17-cv-2989-AT <https://coalitionforgoodgovernance.sharefile.com/d-s7d96b021c2d3419984512b56ff6eee95> (last visited 2 September 2021)

Security Agency (CISA) which issued an advisory warning of the security vulnerabilities.⁹

Still, the Secretary of State has inaccurately assessed the security threats to the BMDs by repeatedly claiming that an attacker could only corrupt one device at a time.^{10, 11} This is incorrect. CISA's vulnerability assessment confirmed Dr. Halderman's findings that there are several vulnerabilities that could be exploited to spread malware from device to device, increasing the impact of an attack.¹² The Secretary's failure to appreciate the gravity and urgency of this breach further imperils Georgia's elections.

Emergency measures can be taken to secure the election and maintain voter confidence.

This newly heightened risk can be mitigated by critical but straightforward action.

First, Georgia should immediately discontinue the universal use of the Dominion ICX BMD for in-person voters, and instead provide voters with emergency hand-marked paper ballots to be tabulated by the current system's optical scanners. Georgia state election rules currently require:

*The Superintendent shall cause every polling place and advance voting location to have a sufficient number of blank paper ballots that can be marked by pen available for use in the event of emergency. The election superintendent shall also be prepared to resupply polling places with emergency paper ballots in needed ballot styles in a timely manner while voting is occurring so that polling places do not run out of emergency paper ballots.*¹³

State rules explicitly direct election officials to prepare for the use of emergency paper ballots, marked by pen. This means all election administrators and pollworkers should *already* be trained in the distribution and use of paper ballots.

⁹ ICS Advisory (ICSA-22-154-01) Vulnerabilities Affecting Dominion Voting Systems ImageCast X, June 3, 2022. Available at: <https://www.cisa.gov/uscert/ics/advisories/icsa-22-154-01>

¹⁰ Mark Neisse, "Handling of Georgia election breach investigation questioned," Atlanta Journal Constitution, September 4, 2022. Available at: [Questions surround handling of election breach investigation in South Georgia county \(ajc.com\)](https://www.ajc.com/news/georgia/2022/09/04/questions-surround-handling-of-election-breach-investigation-in-south-georgia-county-ajc-com/)

¹¹ Emma Hurt, "What's going on with Coffee County?", *Axios*, September 7, 2022. Available at: [2020 election investigation puts a spotlight on Coffee County, GA - Axios Atlanta](https://www.axios.com/2022/09/07/2020-election-investigation-puts-a-spotlight-on-coffee-county-ga-axios-atlanta/)

¹² See *supra* note 9.

¹³ Georgia Rule 183-1-12-.01 Conduct of Elections, Available at: <https://rules.sos.ga.gov/gac/183-1-12>

Georgia counties can scale up their existing procedures to shift the bulk of in-person voting to paper ballots marked by pen. These ballots can be counted by the tabulators currently in use: no new equipment, programming or training is needed.

Voters who need or prefer to mark a ballot with assistive technology can continue to use BMDs with assistive technology. BMD units could also be used as a backup balloting unit if the polling place runs short of a specific ballot style printed ballot. Minimizing the use of the BMDs reduces the threat that BMD tampering can alter election results.

Second, we urge you to use your authority to mandate a *statewide post-election risk-limiting audit (RLA)* of the outcome for all contests on the ballot. Current SEB practice is that only one state-wide contest be audited, every other year; this is insufficient. This proposed audit should be done completely transparently, with citizen observation, under the auspices of local county election officials. Post-election auditing of the outcome requires a trustworthy paper trail of hand-marked paper ballots with limited use of machine-marked ballots.

If a cyberattack, misconfiguration, bug, or procedural lapse changes the outcome, a properly conducted *RLA based on trustworthy paper ballots* will correct the outcome (with high probability). If the election outcome is correct in the first place, the RLA will provide strong public evidence that it is, creating a “firewall” against litigation and disinformation seeking to discredit the outcome.

We believe it is important that a public commitment to rigorous post-election verification be made before Election Day. Otherwise, it may appear to be a partisan decision, and there may be calls for other kinds of “audits” that are neither scientifically grounded nor probative, but could spuriously undermine public confidence in the election. We urge you to take the lead on the auditing issue early and reassure Georgia voters that a thorough transparent audit will promptly follow the election and be completed prior to certifying the results.

In bringing our concerns about the recent Dominion software compromise to your attention we are not accusing Dominion of wrongdoing. Nor do we have evidence that anyone currently plans to hack Georgia’s elections. However, it is critical to recognize that the release of the Dominion software into the wild has measurably increased the risk to the real and perceived security of the election to the point that emergency action is warranted.

We are all willing to discuss any of these points with you or your staff, either in writing or by phone or videoconference. We would be happy to help swiftly design a straightforward, practical, transparent statewide RLA process that will be a model for how elections should be secured. We would like to be helpful in any way that you find useful to defend against the threats posed by the escaped Dominion code and newly discovered Dominion BMD vulnerabilities. Please do not hesitate to call on us to assist.

Yours truly,

Mustaque Ahamad, PhD.
Professor
School of Cybersecurity and Privacy
Georgia Institute of Technology*

Duncan Buell, PhD.
Chair Emeritus — NCR Chair in Computer Science and Engineering
Department of Computer Science and Engineering
University of South Carolina*

Richard DeMillo, PhD.
School of Cybersecurity and Privacy
Charlotte B. and Roger C. Warren Chair in Computing
Georgia Institute of Technology*

Larry Diamond, PhD.
Senior Fellow, Hoover Institution and Freeman Spogli Institute,
Stanford University*

Lowell Finley
Former California Deputy Secretary of State for Voting System Technology and
Policy (2007-2014)

Susan Greenhalgh
Senior Advisor for Election Security
Free Speech For People

David Jefferson, PhD.
Lawrence Livermore National Laboratory* (retired)
Board of Directors, Election Integrity Foundation*

Douglas W. Jones, PhD.
Emeritus Associate Professor of Computer Science
University of Iowa*

Daniel P. Lopresti, PhD.
Professor, Department of Computer Science and Engineering*
President, International Association for Pattern Recognition (IAPR)*
Vice Chair, Computing Research Association's Computing Community
Consortium (CCC)*
Lehigh University*

Mark Ritchie
Former Secretary of State of Minnesota*
Past President National Association of Secretaries of State*

John E. Savage, PhD.
An Wang Professor Emeritus of Computer Science
Brown University*

Kevin Skoglund
President and Chief Technologist
Citizens for Better Elections*

Philip B. Stark, PhD.
Professor, Department of Statistics
University of California, Berkeley*

**Affiliations below are provided for identification purposes only. The statements and opinions expressed here are not necessarily those of our employers or institutions.*



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**



TLP:WHITE

[CISA.gov](#)[Services](#)[Report](#)

Vulnerabilities Affecting Dominion Voting Systems ImageCast

ICS-CERT Advisories > X

ICS Advisory (ICSA-22-154-01)

[More ICS-CERT Advisories](#)

Vulnerabilities Affecting Dominion Voting Systems ImageCast X

Original release date: June 03, 2022

Legal Notice

All information products included in <https://us-cert.cisa.gov/ics> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <https://us-cert.cisa.gov/tlp/>.

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 provides 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>

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

This product is provided subject to this Notification and this Privacy & Use policy.

TLP:WHITE