September 5, 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 Evaluation)

Dear Election Board Members:

Coalition for Good Governance respectfully submits the attached proposed amendments to the State Election Board Rules under the provisions Rule 183-1-1-.01. Original notarized paper copies will be delivered by commercial confirmed delivery. We request that Board members review the electronic copies supplied by email in advance of the receipt of paper copies. Electronic copies also include hyperlinks. We respectfully request that the proposed Rule amendments be heard at the next SEB meeting as required by Rule 183-1-1.01(4).

We submit the proposed rule amendments with the request that the SEB consider the substance and merits of the rule changes and modify or clarify the proposed language and format as appropriate if such edits would facilitate the adoption of the substance and intent of our proposal.

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

(a) The name and post office address of the petitioner;
Mailing address:
Coalition for Good Governance
PO 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(b) The full text of the rule requested to be amended or repealed, or the full text of the rule desired to be promulgated;

Exhibit 1 attached.

(c) The reason(s) such rule should be amended, repealed, or promulgated;

Purpose of Proposed Rules

The purpose of the proposed rules is to provide clear SEB guidance to local election officials as they evaluate the security of their county's voting system equipment, (particularly the vulnerable ICX units), in planning for the 2024 elections. In the proposed rule, we recommend factors for local superintendents to consider in evaluating the security of their equipment and whether, in their judgment, emergency balloting under SEB rules is feasible in some or all of their elections for purposes of mitigating vulnerabilities confirmed in the June 3, 2022 Advisory by the Cybersecurity and Infrastructure Security Agency (CISA) (Exhibit 2). If superintendents conclude that the ICX units are "impossible or impracticable" (in whole or in part) to use in a secure manner without software updates or other cybersecurity mitigations, the secure back up balloting process provided by statute ("emergency ballots") would be used to the extent feasible in upcoming elections. We recommend that the rule be effective for elections between the dates of December 1, 2023 and December 31, 2024. The SEB can reevaluate the rule after the 2024 elections depending on the development and implementation of other mitigation strategies for the CISA-confirmed vulnerabilities and the Coffee County breaches.

Why the Rule is Necessary

In July 2021, Dr. J. Alex Halderman delivered an expert report to this Board and other Defendants in the Curling v Raffensperger lawsuit documenting certain high risk vulnerabilities in the Dominion ICX system components. In June 2022, CISA issued a report confirming Dr. Halderman's findings in the form of an Advisory, entitled *"Vulnerabilities Affecting Dominion Voting Systems ImageCast X."* (Exhibit 2) CISA recommended 13 categories of mitigations be made by election officials using the ImageCast X, although some of those mitigations are not under the control of the local officials. CISA recommended in June 2022 that the documented ***"risks be mitigated as soon as possible.***" However, 14 months after CISA's recommendation, and 26 months after receiving the Halderman report of those vulnerabilities, this Board and the Secretary of State have no plans for even partial mitigation until 2025. It is incumbent on county officials to use their discretion and authority to use hand marked paper ballots to the fullest extent possible in the 2024 elections.

Local election officials may be confused and misled by the so-called "health checks" the Secretary of State is implementing amounting to nothing more than superficial and ineffective testing of the system. As Dr. Halderman writes in a summary of his findings:

"Rather than patching the vulnerabilities, Georgia says it intends to perform security "Health Checks" in each county that will include "verifying HASH [sic] values to verify that the software has not been changed." Such "Health Checks" are unlikely to be an effective countermeasure. At best, verifying hashes ***will only confirm that the equipment is running the vulnerable unpatched software****. And as we explain in the report, malware that has infected the ICX can completely conceal itself from the kind of hash validation performed in Georgia, which relies on the running software to self-attest to its integrity."*

The only truly effective mitigation for the vulnerabilities of the ICX units is to reduce their use by allowing most in-person voters to use hand marked paper ballots, tabulated by the current Dominion scanners and audited with extensive post-election Risk Limiting Audits. The State has announced that it will not undertake ICX updates to partially address such confirmed vulnerabilities. As Dr. Halderman explains, "Announcing this is worse than doing nothing at all, since it puts would-be adversaries on notice that the state will conduct the presidential election with this particular version of software with known vulnerabilities, giving them nearly 18 months to prepare and deploy attacks."

The Secretary of State has disingenuously attempted to rebut the Halderman Report and the CISA findings by promoting the discredited Dominion-sponsored MITRE report with Georgia's local officials. Those local officials have limited information on the failings of the promoted MITRE report, the fact that cybersecurity scientists have called for the retraction of that report, and the concerning results of scientists' meetings with the MITRE representatives to cover the many errors and false assumptions in the report. A recent presentation on the discredited MITRE report was recently made by a panel of experts at DEFCON. (We are happy to supply pdf or paper copies of any of these linked documents upon request.)

Local election officials and the State Election Board have a common interest in promoting trust in the 2024 election – but that trust must be earned through deploying a secure and verifiable system.

Therefore, it is only prudent for the counties to be able to confidently take local action to lessen the extraordinary risk of a cybersecurity attack in the 2024 elections. Georgia's software has been widely distributed to unauthorized actors who can use it to create and deploy undetectable malware for attacking the 2024 elections, exploiting the vulnerabilities that CISA confirmed. It is imperative that local officials evaluate the risks as confirmed by CISA, and determine the feasibility of taking local action to mitigate such risks by using the hand marked paper ballot back-up system in whole or in part, under their local authority to determine whether the voting system is "impracticable or impossible" to utilize. The fewer the BMD units in operation in the county, the more secure the election.

Local superintendents need SEB guidance to clarify their existing local statutory authority to undertake the risk evaluation and the authority to elect to implement the back-up balloting system without fear of improper enforcement action from the SEB. Local officials need such guidance to ensure that the SEB will not attempt to enforce statewide uniformity of the use of ICX's in 2024, despite county officials' existing authority to determine if the system is "impossible or impracticable" to use in light of the current cybersecurity risks. Superintendents also need guidance to permit the adoption of mitigation solutions to remove as many ICX units as feasible without a requirement to adopt an "all or none" ICX policy as they attempt to mitigate, or partially mitigate, the vulnerabilities of the system.

(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 secure ballot. Members' particular circumstances and election risk exposure may vary from voter to voter. Therefore, it is infeasible to present "all pertinent existing facts as to the petitioner's interest in the matter."

Coalition for Good Governance is a plaintiff in the Curling v Raffensperger case in which members of this Board are Defendants.

(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

All Georgia voters and candidates likely benefit by adoption of a proposed rule vindicating Georgia voters' federal and state legal rights to voting a secure and accountable ballot that is resilient to actual or fabricated accusations of outcome-changing vote tampering.

Additionally, election officials at the municipal, county, and state level may choose to undertake different procedures than those used at present to ensure voting system security through hand marked paper ballots. Such measures would affect officials' activities in the polling places. Switching to secure emergency ballots, when implemented, should substantially *reduce the complexity and cost of conducting elections* when using hand marked paper ballots, counted by Dominion scanners. Local election officials would benefit from clearer rules as they have received mixed messages about use of emergency balloting and their local authority to make the determination when the use of BMDs is "impossible or impracticable."

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

Citations of applicable law: O.C.G.A. §21-2-334; O.C.G.A. §21-2-281; SEB Rule 183-1-12-.04;

Authority of SEB to promulgate election rules:

In the past, the SEB has cited the uniform voting system requirements in O.C.G.A. §21-2-300(a) as providing no leeway for SEB to promulgate rules addressing circumstances that make it inappropriate to use BMDs. The statute clearly anticipates that there may be exceptions to the uniform universal use of BMDs in its provision "unless otherwise permitted by law." It is also essential to understand that the BMD required to be installed by §21-2-300(a) is ***not*** the system now operating in Georgia. (See Exhibit 3)

Georgia statutes permit hand marked paper ballots when the voting equipment is "impossible or impracticable" to use. Controlling statutes O.C.G.A. §21-2-281 and §21-2-334 make no mention of "emergency situations," nor do they require a suddenly discovered, unanticipated event to trigger the need to use the back-up paper balloting system. There are numerous examples of SEB election rules providing exceptions from the use of the otherwise uniform voting system equipment. For example, SEB Rules dictate that when polling place "zero tapes" show vote tallies, the scanners, although physically "possible" to use, shall not be used (because of the risk of wrong election results). The SEB rules also permit use of hand marked paper ballots in the event that voting lines exceed 30 minutes, despite the fact that machines are not "impossible" to use in that case. SEB recount rules require a hand recount, avoiding the voting system scanners, if the recount Logic and Accuracy testing is unsuccessful. This Board has often recognized in its rule-making that the statutes authorizing voting systems are not to be read to require equipment use on an unconditional and illogical basis, regardless of the risks or impact on election integrity, security, accuracy or fairness.

The risk of cyberattacks is quite real, and local county officials have the means, authorized by statute, to thwart outcome-changing attacks. They should be encouraged to do so and their work facilitated by prudent SEB rules focused on the 2024 elections.

The zealous protection of election security is essential. The use of BMDs is not.

Additional information

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 privacy risks to in-person voters in 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 the practice of hearing such rule-making petitions at prior SEB meetings.

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

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 September 5, 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 7th day of September 2023.

Marilyn Marks

Sworn to and subscribed before me
This 7 day of September 2023.

O'Hagi M. McGriff
Notary Public
Mecklenburg County, NC
My Commission Exp 05/21/2026

Exhibit 1 - 1

Red font indicates new text.

Blue font indicates deleted text.

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

Exhibit 2

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 the use of electronic ballot markers is determined to be impossible or impracticable, 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.

Exhibit 1 - 3

(d)) If ~~an emergency situation exists that makes voting on~~ the use of electronic ballot markers is determined to be impossible or impracticable, the poll manager shall alert the election superintendent as soon as possible. The ~~existence of an emergency situation~~ determination shall be in the discretion of the election ~~supervisor~~ superintendent. 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, or designee, shall either overrule or concur with the declaration of ~~emergency~~ such circumstances. While the determination of ~~an emergency situation~~ situations requiring back up balloting based on the BMD use being "impossible or impracticable," is in the discretion of the election superintendent, the types of events that may be considered ~~emegencies~~ are power outages, malfunctions causing a sufficient number of electronic ballot markers to be unavailable for ~~use~~ legal compliance with applicable laws and rules, cybersecurity risks, or waiting times longer than 30 minutes.

(e) After conducting a diligent review of the June 3, 2022 Cybersecurity and Infrastructure Security Agency (CISA) Advisory, *Vulnerabilities Affecting Dominion Voting Systems ImageCastX,* and its recommended mitigations, the superintendent may, in their discretion, determine that it is impossible or impracticable to adequately secure the electronic ballot marking system for some or all of the county's in-person voting for any primary, special, runoff or general elections, for such elections conducted

Exhibit 4

between December 1, 2023 and December 31, 2024, provided that electronic ballot marking devices are available for voters requesting such assistive technology. Any such determination shall be made during a noticed public meeting, allowing appropriate opportunity for public comment. Upon such a determination, emergency ballots shall be used as provided in this paragraphs (c) and (d) of this section.

(i) In making such determination, the superintendent may also consider the feasibility of fully complying with BMD Logic and Accuracy Testing requirements of O.C.G.A. §21-2-379.25 (c), mandating that *each* BMD must be tested for *every* candidate in *every* contest and every ballot question for all ballot styles. Other security factors that may be considered in such determination include, but are not limited to, 1) adequacy of the physical security of the ICX units since initial adoption, including the vigilant use of tamper evident seals and locks, 2) historic adequacy of the chain of custody of the ICX units since initial adoption, 3) adequacy of the historic practices of avoiding direct or indirect internet connection to any ICX devices or the EMS server, 4) the planned scope of voluntary post-election audits, 5) the ability to continuously and robustly monitor the ICX units in polling places after set up, (6) the risk posed by the 2021 state voting system breaches initiated in Coffee County, and 7) whether Democracy Suite version 5.17 (or later) has been installed on the counties' voting systems. The superintendent shall consider such factors as the feasibility of the use of emergency balloting including worker training and

Exhibit 13

voter education to ensure the smooth operation of voting without voter confusion, and the prevention of ballot style issuance errors. Superintendents may choose to conduct all or part of the elections using emergency balloting based on local implementation feasibility considerations.

(f) Emergency ballots used in all voting locations may be printed by mobile ballot printing applications or by commercially pre-printed ballots or a combination of both, maintaining strict ballot accounting controls required by statute and rules. Black ballot marking pens shall be supplied in each voting station for marking such emergency ballots.

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,

Exhibit 1 6

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.

Exhibit 17

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

Exhibit 8

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 thc ballot prcscntcd 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 neccssary 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

Exhibit 1 - 9

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

Exhibit 10

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.

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.

Exhibit 2-1

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

Exhibit 2-2

- 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

Exhibit 2-3

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.

Exhibit 2-4

- 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.

Exhibit 3

Dominion BMD (5.5-A and 5.17) Does Not Meet General Assembly's BMD Requirements

HB316 Required	**Dominion BMD System Violation**	**Citation**
"Absolute ballot secrecy" for any BMD system adopted or used.	Touchscreen display shows voters' selections to others in polling place.	O.C.G.A. §21-2-379.22(5) **(HB316)**
BMD must allow voter to "privately mark a ballot."	Touchscreen displays show voters' selections violating the privacy requirement.	O.C.G.A. §21-2-2(7.1) **(HB316)**
GA Constitutional right to cast a secret ballot	Touchscreen display shows voters' selections to others in polling place.	Ga. Const. art. II, § 1,¶1
Voter must be able to "verify (in a private and independent manner) the votes selected by the voters on the ballot before the ballot is cast and counted."	Voter cannot verify the votes selected (because of QR codes) Voters not permitted privacy in reviewing their touchscreen votes.	Federal law 52 USC §2108(a)(A)(i)
Voter must be able "to change the ballot or correct any error before the ballot is cast and counted,"	Voters cannot correct a machine marking error as voter cannot read the QR code to detect error.	Federal law 52 USC §2108(a)(A)(ii)
Requirement for an "elector-verifiable paper ballot."	Voter cannot verify the machine-marked vote encoded in QR code.	O.C.G.A. §21-2-2(7.1) **(HB316)**
Ballot must be "marked with the elector's choices in a format readable by the elector."	Voter cannot read the vote choices that are counted.	O.C.G.A. §21-2-379.22(6) **(HB316)**
The system must be "safe and practicable for use."	System is not practicable when it violates state and federal law. System is not safe given the confirmed vulnerabilities in the Halderman report.	O.C.G.A. §21-2-300(a)(1) **(HB316)**
The system can be "safely and accurately used by electors."	System is not secure as accuracy in question as confirmed in Halderman report.	O.C.G.A. §21-2-379.24 **(HB316)**
In every election, "***each*** BMD must be tested to ascertain that it will correctly record the votes cast for all offices and on all questions…" (Logic & Accuracy Testing)	State says that the required testing is not feasible and too time consuming. Current procedure does not conduct compliant testing.	O.C.G.A. §21-2-379.25(c) **(HB316)**