

From: Commissioner Jerdonek  
Date: June 26, 2023

Subject: Public Release of July 2021 Halderman Report on Security Problems Affecting  
Dominion's Voting System

The purpose of this memo is to provide a recent update related to a January 28, 2022 letter that then-President Bernholz wrote to the California Secretary of State on behalf of the Elections Commission about a then-sealed report on security vulnerabilities in Dominion's voting system.

### **Background**

At the Commission's January 19, 2022 meeting, the Commission discussed a letter that Dr. David Jefferson wrote to the Commission on January 2, 2022. Dr. Jefferson's letter was about a report that Dr. J. Alex Halderman co-wrote about security vulnerabilities he discovered in Dominion's ImageCast X voting system. Dr. Halderman prepared his report for a federal court case called *Curling v. Raffensperger* in the Northern District of Georgia.

In his letter, Dr. Jefferson explained to the Commission that the Court decided not to allow Dr. Halderman's report to be made public (i.e. it had to remain sealed). However, because of the seriousness of the vulnerabilities and the fact that San Francisco could be subject to those vulnerabilities because San Francisco uses Dominion's voting system, Dr. Jefferson encouraged the Commission to request a copy of the sealed report, which it had the right to do.

Following the discussion, the Commission voted unanimously to authorize President Bernholz to forward to the California Secretary of State the information that Dr. Jefferson provided to the Commission, to urge her to investigate the matter, and to request acknowledgment. President Bernholz's January 28, 2022 letter (with Dr. Jefferson's letter and attachments themselves attached) can be found on the Commission's Letters page.<sup>1</sup>

Note that the vulnerabilities covered by the above report are different from the DVSSorder privacy flaw in Dominion's voting system that Dr. Halderman separately discovered and wrote to the Commission about on January 9, 2023. (The Commission discussed DVSSorder at the Commission's February 15, 2023 meeting,<sup>2</sup> at which Dr. Halderman was a guest speaker, as well as at subsequent meetings.)

[continued next page]

---

<sup>1</sup> <https://sf.gov/resource/2022/elections-commission-letters>

<sup>2</sup> <https://sf.gov/meeting/february-15-2023/elections-commission-regular-meeting>

## **Update**

To my knowledge, the Secretary of State never replied to the Commission's January 28, 2022 letter.

However, the recent development is that on June 14, 2023, the U.S. District Court for the Northern District of Georgia finally decided to allow Dr. Halderman's report to be made public. The 96-page report is dated July 1, 2021 and is called, "Security Analysis of Georgia's ImageCast X Ballot Marking Devices."

Attached to this memo is a PDF print-out of a June 14, 2023 blog post<sup>3</sup> that Dr. Halderman wrote describing the events and information surrounding his 96-page report. The first paragraph of the blog post also contains a link to the original, now-unsealed report.

## **Attachments**

1. "Security Analysis of the Dominion ImageCast X" (10 pages)

---

<sup>3</sup> <https://freedom-to-tinker.com/2023/06/14/security-analysis-of-the-dominion-imagecast-x/>

# Freedom to Tinker

Research and commentary on digital technologies in public life

## Security Analysis of the Dominion ImageCast X

JUNE 14, 2023 BY J. ALEX HALDERMAN

**J. Alex Halderman** is Professor of Computer Science & Engineering at the University of Michigan and Director of Michigan's **Center for Computer Security & Society**. He has twice testified to Congress about election cybersecurity, and he co-chairs the State of Michigan's Election Security Advisory Commission. His course on election technology, **Securing Digital Democracy**, is available on Coursera.

Today, the U.S. District Court for the Northern District of Georgia **permitted** the public release of **Security Analysis of Georgia's ImageCast X Ballot Marking Devices**, a 96-page report that describes numerous security problems affecting Dominion voting equipment used in Georgia and other states.

I prepared the report two years ago, together with Prof. **Drew Springall** of Auburn University, as part of a long-running voting-rights lawsuit, **Curling v. Raffensperger**. Back in September 2020, the Court **granted** the *Curling* Plaintiffs access to one of Georgia's touchscreen ballot marking devices (BMDs) so that they could assess its security. Drew and I extensively tested the machine, and we discovered vulnerabilities in nearly every part of the system that is exposed to potential attackers. The most critical problem we found is an arbitrary-code-execution vulnerability that can be exploited to spread malware from a county's central election management system (EMS) to every BMD in the jurisdiction. This makes it possible to attack the BMDs at scale, over a wide area, without needing physical access to any of them.

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

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

Beyond these implications for election practice, our work is scientifically significant. It is the first study in more than 10 years to comprehensively and independently assess the security of a widely deployed U.S. voting machine, as well as the first-ever comprehensive security review of a widely deployed ballot marking device. Security researchers studied numerous U.S. voting machines 10-20 years ago, and their findings **clearly established** that voting equipment tends to suffer from security flaws. Yet one might wonder whether election equipment sold today is

Freedom to Tinker is hosted by Princeton's **Center for Information Technology Policy**, a research center that studies digital technologies in public life. Here you'll find comment and analysis from the digital frontier, written by the Center's faculty, students, and friends.

### What We Discuss

- AACS bitcoin CD Copy Protection censorship CITP **Competition**
- Computing in the Cloud **Copyright**
- Cross-Border Issues cybersecurity policy
- DMCA DRM** Education ethics
- Events Facebook FCC Government
- Government transparency Grokster
- Case Humor **Innovation Policy**
- Internet Law **Managing the Internet Media** NSA Online
- Communities **Peer-to-Peer**
- Predictions **Princeton Privacy**
- Publishing Recommended Reading
- Secrecy **Security** Spam Super-DMCA surveillance Tech/Law/Policy
- Blogs **Technology and Freedom** transparency
- Voting** Wiretapping WPM

### Contributors

### Archives by Month

- o 2023: J F M A M J J A S O N D
- o 2022: J F M A M J J A S O N D
- o 2021: J F M A M J J A S O N D
- o 2020: J F M A M J J A S O N D
- o 2019: J F M A M J J A S O N D
- o 2018: J F M A M J J A S O N D
- o 2017: J F M A M J J A S O N D
- o 2016: J F M A M J J A S O N D

more secure than equipment produced in decades past. Our findings suggest that the answer is no. This highlights the need for further enhancements to the software engineering, testing, and certification processes for U.S. voting equipment, and it underscores the importance of conducting rigorous post-election audits of every major electoral contest, as recommended by the [National Academies](#).

Drew and I are grateful to the *Curling* Plaintiffs and their legal team for the opportunity to perform this work. We also thank the numerous experts who helped [explain to the Court](#) why making the report public now is responsible disclosure that [serves the public's interest](#). Adversaries seeking to attack election systems can readily discover the same or similar problems in the Dominion ImageCast X, but unsealing the report will help equip election officials and other policymakers with the information they need to mount an effective response.

[You can read the previously-sealed “Halderman and Springall Report” here.](#)

There have been many developments in the two years since the report was written. The rest of this post will provide important context for understanding the findings and their implications for election security and public policy.

## What is the *Curling* lawsuit?

Since 2017, concerned voters and [advocates](#) have been challenging parts of Georgia’s election technology in federal court. Their lawsuit, *Curling v. Raffensperger*, started when Georgia still used Diebold paperless touchscreen voting machines. A decade earlier, I helped California’s Secretary of State conduct [a landmark security review](#) that discovered ways to infect the same Diebold models with vote-stealing malware (among other problems). California responded by decertifying the Diebold system, but Georgia used it statewide through the end of 2019 *without even patching the security flaws*. After extensive expert testimony about the vulnerability of the Diebold equipment, Judge Amy Totenberg [ordered Georgia](#) to replace the machines by the beginning of 2020.

Ignoring advice from election security experts, including the lone cybersecurity expert on the Governor’s commission to recommend a new voting system, Georgia replaced the Diebold machines with a new voting system that is centered around the [Dominion ImageCast X](#) (ICX) ballot-marking device. Voters use the BMD to make selections on a touchscreen and print a marked ballot, which is then scanned and counted by a separate machine. In most of the U.S., voters mark ballots by hand, and BMDs like the ICX are reserved as an assistive technology for voters who need them. Georgia, by contrast, is one of [only two states](#) where *everyone* who votes in-person is required to use a BMD statewide. This arrangement, called “universal-use BMDs”, [creates security risks](#) by placing a potentially hackable computer between voters and their ballots. Because of these security concerns, the *Curling* suit continued, and the Plaintiffs are now challenging Georgia’s universal-use BMD system.

- o [2015: J F M A M J J A S O N D](#)
- o [2014: J F M A M J J A S O N D](#)
- o [2013: J F M A M J J A S O N D](#)
- o [2012: J F M A M J J A S O N D](#)
- o [2011: J F M A M J J A S O N D](#)
- o [2010: J F M A M J J A S O N D](#)
- o [2009: J F M A M J J A S O N D](#)
- o [2008: J F M A M J J A S O N D](#)
- o [2007: J F M A M J J A S O N D](#)
- o [2006: J F M A M J J A S O N D](#)
- o [2005: J F M A M J J A S O N D](#)
- o [2004: J F M A M J J A S O N D](#)
- o [2003: J F M A M J J A S O N D](#)
- o [2002: J F M A M J J A S O N D](#)

[author log in](#)



The Dominion ICX BMD consists of an off-the-shelf tablet and laser printer.

In September 2020, the Court **authorized** the Plaintiffs to test the security of the BMD system, subject to strict protocols, including a **protective order** to ensure confidentiality and continuous video monitoring. The Curling Plaintiffs commissioned Drew and me to perform their security review. We were provided a Dominion ImageCast X (ICX) BMD and a Dominion ImageCast Precinct (ICP) ballot scanner, both configured as they would be used in a real election in Georgia. We were also provided access tokens and passwords that allowed us to operate the equipment as poll workers would and conduct mock elections. (Contrary to the **Georgia Secretary of State's spin**, providing such passwords is a routine part of security testing. The passwords are not necessary to compromise the equipment, because, as our report explains, there are several ways that attackers can bypass them.) I submitted an expert report describing our findings under seal with the Court on July 1, 2021, and it has remained confidential until now.

*Curling* Plaintiffs, Secretary Raffensperger, Dominion, and CISA have all asked that the report be unsealed. Last week, the Court **authorized** its public release, with a few narrow redactions that Drew and I proposed to withhold key technical details that would benefit attackers. It was posted on the public docket today.

## What vulnerabilities did you find?

The ICX is a commercial off-the-shelf (COTS) tablet computer running the same Android operating system used in devices like mobile phones. The voting functions are provided by a custom app written by Dominion. Georgia's version of the software (Democracy Suite 5.5-A) uses Android 5.1.1, which has not been updated (even to address security vulnerabilities) since 2015.

We applied an open-ended vulnerability testing methodology, in which we assumed the role of an attacker and attempted to find ways to compromise the system. Over approximately 12 person-weeks of investigation, we found vulnerabilities in practically every significant attack surface and developed several proof-of-concept attacks to exploit them.

The most critical vulnerability we found is a software flaw that would allow an attacker to spread malware from a county's central election management system (EMS) computer to every ICX in the jurisdiction. Before an election, workers use the EMS to prepare an *election definition*—data files that describe what's on the ballot—and they copy this data from the central computer to every ICX using USB sticks. We discovered a vulnerability in the ICX software that loads the election definitions. By modifying the election definition file in a precise way, an attacker can exploit the vulnerability to install arbitrary malicious code that executes with root privilege when the ICX loads the election definition. The underlying problem is a classic “Zip Slip” vulnerability (in which a modified .zip file can overwrite arbitrary filesystem paths when it is decompressed), coupled with a badly designed system-level service that facilitates privilege escalation.

This attack is especially dangerous because it is *scalable*—a single intrusion to the EMS computer in a county office could affect equipment in polling places over a very wide area.

***Attackers do not need access to each individual machine.***

EMSs are supposed to be well secured, and in most (but not all) states they are not supposed to be connected to outside networks. However, they are vulnerable to attacks by election insiders—or outsiders with insider assistance. Following the November 2020 election, local officials in several states, including Georgia, gave potentially untrustworthy outsiders physical access to their EMSs and other equipment. This is exactly the sort of access that would enable the attack I've just described (and many other attacks as well).

We also discovered a wide variety of other vulnerabilities in the ICX. I encourage you to read the full report for details, but here are a few examples:

- The ICX doesn't appropriately limit what kinds of USB devices can be plugged in, and it does not adequately prevent users from exiting the voting app. As a result of a botched Dominion software update installed by Georgia, anyone can attach a keyboard and press alt+tab to access Android Settings, then open a root shell or install arbitrary software. We show that this could even be exploited by a voter in the voting booth, by reaching behind the printer and attaching a USB device called a Bash Bunny to the printer cable.
- The ICX uses smartcards to authenticate service technicians, poll workers, and voters, but the smartcard authentication protocol is completely broken. Attackers can create counterfeit technician cards that give them root access to the machine, steal county-wide cryptographic secrets from access cards used by poll workers, and create “infinite” voter cards that allow an unlimited number of ballots.
- The ICX ships with a text editor and a terminal emulator that allows root access. Anyone with access to an ICX can use these apps to tamper with all of the machine's logs and protective counters, using only the on-screen keyboard.

The breadth of these problems speaks to the generally poor quality of software engineering that went into the ICX, and the lax security standards under which it was tested and certified.

## **Isn't there a paper trail? Why is malware a risk?**

Here is an example of a ballot produced by an ICX in Georgia. It will help illustrate what an attacker could potentially do by installing malware on the BMDs. Notice that the voter's selections are printed as a long list of small text at the bottom of the page. The computer scanners that count the ballots ignore that text. Instead, the votes they count come entirely from data in the QR code (the square barcode in the middle of the page).



**FAYETTE COUNTY  
OFFICIAL BALLOT  
GENERAL AND SPECIAL ELECTION  
OF THE STATE OF GEORGIA  
NOVEMBER 3, 2020**

*"I understand that the offer or acceptance of money or any other object of value to vote for any particular candidate, list of candidates, issue, or list of issues included in this election constitutes an act of voter fraud and is a felony under Georgia law." [O.C.G.A. 21-2-284(e), 21-2-285(h) and 21-2-383(a)]*

376-Shakerag East



For President of the United States (Vote for One) (NP) Vote for Donald J. Trump (I) (Rep)	For State Representative In the General Assembly From 72nd District (Vote for One) (NP) Vote for Josh Bonner (I) (Rep)	For County Commissioner District 5 (Vote for One) (NP) Vote for Charles W. Oddo (I) (Rep)
For United States Senate (Perdue) (Vote for One) (NP) Vote for David A. Perdue (I) (Rep)	For Judge of the Probate Court (Vote for One) (NP) Vote for Ann S. Jackson (I) (Rep)	For County Board of Education District 1 (Vote for One) (NP) Vote for Randy Hough (Rep)
For United States Senate (Loeffler) - Special (Vote for One) (NP) Vote for Kelly Loeffler (I) (Rep)	For Clerk of Superior Court (Vote for One) (NP) Vote for Sheila Studdard (I) (Rep)	For County Board of Education District 5 (Vote for One) (NP) Vote for Brian Anderson (I) (Rep)
For Public Service Commissioner (Vote for One) (NP) Vote for Jason Shaw (I) (Rep)	For Sheriff (Vote for One) (NP) Vote for Chris Pigors (Dem)	Constitutional Amendment #1 (NP) Vote for YES
For Public Service Commissioner (Vote for One) (NP) Vote for Nathan Wilson (Lib)	For Tax Commissioner (Vote for One) (NP) Vote for Kristie King (I) (Rep)	Constitutional Amendment #2 (NP) Vote for NO
For U.S. Representative in 117th Congress From the 3rd Congressional District of Georgia (Vote for One) (NP) Vote for Drew Ferguson (I) (Rep)	For Coroner (Vote for One) (NP) Vote for W. Bee Huddleston (I) (Rep)	Statewide Referendum A (NP) Vote for NO
For State Senator From 16th District (Vote for One) (NP) Vote for Marty Harbin (I) (Rep)	For Solicitor-General (Vote for One) (NP) Vote for James K. Inagawa (I) (Rep)	Fayette Co School District Homestead Exemption - Special (Vote for One) (NP) Vote for NO
	For County Commissioner District 1 (Vote for One) (NP) Vote for Eric K. Maxwell (I) (Rep)	

1/1

*An ICX ballot. Ballot scanners count the votes in the QR code, not the text.*

An attacker who wants to change votes has two good strategies: (1) Change only the data in the QR code; or (2) Change *both* the QR code and the text, in a way that agrees. The vulnerabilities we found would let an adversary carry out either attack by tampering with the ICX's software.

If an attacker changes only the QR code, voters have no way to detect the change by looking at their ballots, since voters can't read the QR code. The change *might* be detected in a manual recount or a risk-limiting audit (RLA) based on a review of the printed text, but that is unlikely given Georgia's weak audit requirements, which have **recently been further diluted**. Absent a rigorous audit of the paper ballots for the affected contest, this style of attack could change an election outcome without detection.

The other possible attack strategy is to change *both* the QR code and the ballot text. In that case, there's no possibility for an audit to detect the fraud, since all records of the vote will be wrong. Only voters could detect the fraud, by carefully reviewing the printed ballot text and raising alarms if it didn't match their intended selections. This is a problem, because we know that only a small fraction of voters carefully review their ballots. My students and I **ran a mock election** with BMDs that we secretly hacked to change one vote on every printout, yet only about 6% of our test voters reported the errors. Real voters probably wouldn't fare much better. In a study commissioned by the Georgia Secretary of State's Office, University of Georgia

researchers **observed BMD voters** during the November 2020 election. Even when poll workers prompted the voters to review their ballots, 51% barely glanced at them, and less than 20% inspected them for even 5 seconds. The ballot image above is from that same election. How long does it take you just to spot that one selection is for a Democrat?

If voters themselves don't detect the errors on the printed ballot, there's no other way to reliably catch cheating that changes both the QR code and the text. Auditing after-the-fact wouldn't help, because all records of the vote would be wrong in a way that matches. And even if some voters complained that their BMDs did not record their votes correctly, what could officials do? In a close election (say, a margin of 0.5%), given realistic ballot verification rates, the BMDs could alter enough ballots to change the outcome while raising an average of less than one voter complaint per polling place. There would be no ready way for officials to tell whether those who complained were lying, telling the truth, or simply mistaken. Yet there'd also be no way to correct the outcome without rerunning the election. Election officials would have **no good options**.

## Are other states affected?

Beyond Georgia, the ICX is used in parts of 16 other states. Most states use it as an optional assistive device that is used by only a small fraction of voters, which is relatively low risk. However, the ICX can also be used as a DRE voting machine, either with or without a paper trail. In this mode, votes are recorded in an electronic database on the ICX, rather than being scanned from the paper by a separate device. Louisiana uses the ICX statewide for early voting as a paperless DRE. In Nevada, most counties use the ICX as a DRE with a paper trail. Many of our findings likely affect the ICX in DRE-mode too, which would be extremely dangerous, but we have not been granted the necessary access to test the machine in DRE configurations.

## How were these problems disclosed to officials?

Counsel for Georgia's Secretary of State received the report when I submitted it on July 1, 2021. In December 2021, the Court directed the parties to share the report with Dominion so that the company could begin mitigating the vulnerabilities to the extent possible. In February 2022, at the request of the Curling Plaintiffs, the Court **allowed me and Drew** to communicate the report to CISA's coordinated vulnerability disclosure (CVD) program so that other states that use the same equipment could be notified about the problems. CISA validated the vulnerability findings and issued a public **security advisory** on June 3, 2022.

CISA's advisory lists nine individual security flaws (CVEs) affecting the equipment. It concludes that "these vulnerabilities present risks that should be mitigated as soon as possible" and recommends a range of mitigations to "reduce the risk of exploitation." However, unlike the expert report made public today, CISA's advisory contains few details about the problems, giving states and experts not involved in the litigation little information to understand why the mitigations are important or to prioritize their implementation. The release of the full report helps close this gap, permitting election officials to understand why rapid mitigation is essential.

Following our disclosure, Dominion produced a new software version, **Democracy Suite 5.17**, that purportedly addresses several of the vulnerabilities described in the report (the update also addresses the **DVSorter vulnerability**, a serious privacy flaw in Dominion ballot scanners that my students and I discovered outside the context of *Curling*). The patched software entered federal certification testing in October 2022 and was certified by the U.S. Election Assistance Commission on March 16, 2023. Drew and I do not have access to the updated software (nor, to our knowledge, does CISA), so we cannot verify whether the changes are effective. It's also important to note that our findings suggest there are probably other, equally serious vulnerabilities in the ICX that have yet to be discovered.

## Are the machines and software physically secured?



States attempt to control access to voting equipment, but their protections are not always effective.

In early 2021, the ICX software used throughout Georgia **was stolen** and widely distributed by unauthorized parties after local election insiders gave them **repeated access to the election management system and voting equipment** in at least one Georgia county for a period of weeks. This access, which first came to light due to the *Curling* lawsuit, would have been sufficient to let malicious parties develop and test attacks that exploit any of the vulnerabilities that Drew and I discovered, and potentially other vulnerabilities that we missed. Kevin Skoglund and I each analyzed forensic evidence from this breach for the *Curling* case, and we explained its security implications in a pair of **expert reports**.

Related breaches of local election offices occurred in **Michigan** and in **Colorado**, and similar incidents **may well happen again**.

Further evidence about the physical security of voting equipment in Georgia comes from a **2021 memo** (obtained under an open-records request) written by the recently hired election director of Coffee County. He describes how, under his predecessor, the county's Dominion equipment was "stored in a room with an unlocked door to the outside of the building, a leaking roof, and walls with sunlight streaming through crevices."

## COFFEE CO BOARD OF ELECTIONS & REGISTRATION

224 W Ashley St  
DOUGLAS, GA 31533

Ernestine Thomas-Clark, Chairman  
Andy Thomas, Board  
Eric Chaney, Board

(912) 384-7018  
FAX (912) 384-1343

James Barnes, Election Supervisor  
Wendell Stone, Board  
Matthew McCullough, Board

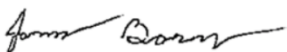
To whom it may concern,

I took over operations at the Coffee County Board of Elections & Registration on April 1<sup>st</sup> 2021. The office had been closed, and locked, since February 2021. Election materials that should have been turned over to the Clerk of Court dating from 2019 were scattered throughout the office. Documents dating as far back as 2010 were stored in a room with a leaking roof, walls and no environmental controls. Confirmation cards, precinct cards, and a large number of drivers licenses were found that had not been mailed to voters.

Coffee ICPs were stored in a room with an unlocked door to the outside of the building, a leaking roof, and walls with sunlight streaming through crevices. Pollen and dust coated the equipment and there was evidence of water accumulation. Back-up battery UPSs were stacked two, three, and four high. The faces of units were detached, and all units were tied to carts using their power cord. Memory cards from the previous voting equipment had not been turned over to CES.

Cast ballots from multiple elections were mixed together in stacks and piles throughout the office. Absentee by mail envelopes from multiple elections were similarly strewn about the office in scattered piles. Most of the BMDs, printers, and UPSs had never been unboxed or inventoried. The routine maintenance, and charging, of equipment had not been performed and documented. There was also no color printer, camera, blue back drop, or TVIC sheets for the Voter ID system.

Regards  
James A Barnes, Jr.  
Coffee County  
Board of Elections & Registration



## What has Georgia done to mitigate the problems?

Although Georgia Secretary of State Brad Raffensperger has had access to our findings for nearly two years, we are unaware of any effective steps the Secretary's Office has taken to address the vulnerabilities. In particular, it has not implemented the mitigations **prescribed by CISA**.

Instead, Secretary Raffensperger recently announced that Georgia will not install Dominion's security patches **until after the 2024 presidential election**. 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.

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.

## Didn't MITRE assert that exploiting the ICX is impractical?

In March 2022, Dominion hired MITRE to respond to our report. Dominion did not give MITRE access to the voting equipment or software, so, unlike us, they couldn't perform any actual security tests. Instead, MITRE assessed the attacks described in our report without essential access to the source information.

MITRE's analysis, which is unsigned, applies faulty reasoning to assert that exploiting the vulnerabilities is "operationally infeasible." This contradicts **CISA's determination** that "these vulnerabilities present risks that should be mitigated as soon as possible."

MITRE's entire analysis is predicated on an assumption known to be wrong. As noted on the first page of the document, "MITRE's assessment of the researcher's proposed attacks **assumes strict and effective controlled access** to Dominion election hardware and software." That assumption was ill-considered when it was written, and it is ridiculous today, since we now know that the Georgia ICX software has already been **stolen and widely distributed** and that election equipment in at least one Georgia county was **repeatedly improperly accessed**. It is not credible to expect that Georgia will perfectly protect its election equipment from illicit access across all 159 counties.

MITRE's analysis isn't simply wrong—it is dangerous, since it will surely lead states like Georgia to postpone installing Dominion's software updates and implementing other important mitigations. In light of the overwhelming evidence of physical security lapses in Georgia and other states, MITRE should retract the report, which fails to account for the real-world conditions under which election equipment is stored and operated.

**Update (2023/06/16):** More than 25 leading experts in cybersecurity and election security have **sent a letter** to MITRE CEO Jason Providakes urging him to retract MITRE's dangerously mistaken report.

## What does EAC say about these problems?

A further implication of our findings is that current U.S. election system testing and certification does not produce adequately secure technology. The ICX was repeatedly tested by federally accredited labs and certified by the U.S. Election Assistance Commission (EAC) and by several states, including Georgia, but we still managed to find vulnerabilities throughout the system. What's more, **EAC has stated** that none of the vulnerabilities we reported—including the arbitrary-code-execution flaw—violate the applicable certification requirements!

#### EAC Findings and Resources

The EAC has reviewed the draft CISA advisory and concurs with their suggested mitigations and notes that most of these mitigations follow generally accepted best practices for securing election systems, maintaining strong chain of custody, and performing pre- and post-election audits as previously published and endorsed by the EAC: <https://www.eac.gov/election-officials/election-security-preparedness>.

Additionally, the EAC's review of the CISA advisory and underlying security researcher's report has not identified any non-conformities with the Voluntary Voting System Guidelines (VVSG) under which this component was certified. Help America Vote Act of 2002, 52 U.S.C. §§ 20922(5), 20971(b)(1) (2022). Decertification actions against this system are not being pursued. The EAC stands ready to accept and expedite processing of any software patches made available by the voting system manufacturer to further protect against exploitation of any identified vulnerabilities.

This highlights the need to significantly strengthen federal certification. One important reform is to require rigorous, adversarial-style penetration testing, which legislation recently introduced by Senators **Warner and Collins** seeks to do. Another important step is to decertify vulnerable software versions once security updates are available, so that states have the impetus to promptly install such fixes.

Reforms like these are urgent, because our findings suggest a systemic failure in voting system design and regulation. The engineering processes that produced the ICX clearly did not give sufficient priority to security, and the result is a brittle system, which we fully expect has additional, similarly serious problems left to be found. We also expect that there are similar problems in voting equipment and software from other manufacturers, who operate under the same regulations and incentives as Dominion, but whose equipment has yet to receive the same intense public scrutiny.

## Does this prove the 2020 election was stolen?

No, of course not.

As **I and other election security experts** wrote in November 2020, “no credible evidence has been put forth that supports a conclusion that the 2020 election outcome in any state has been altered through technical compromise.” That remains true today. The equipment we tested for the Curling lawsuit did not contain data from past elections, so our investigation could not have uncovered traces of real-world attacks, and we are not aware of any evidence that the vulnerabilities we found were ever exploited maliciously. However, there *is* a real risk that they will be exploited in the future unless states like Georgia do more to safeguard elections.

For exactly that reason, we urge those working to debunk election conspiracy theories to carefully distinguish between claims that the 2020 U.S. election result was hacked—for which there is no evidence—and claims that U.S. elections have real vulnerabilities and face threats from sophisticated attackers—which is the **consensus view of the National Academies**. Failure to clearly maintain this distinction confuses the public, discredits anti-disinformation efforts, and makes it even more difficult to have important public conversations about vital election security reforms and to implement those reforms. Voters deserve better.

## Will these findings make voters less confident?

## What should be done to fix the problems?

We're sorry to be the bearers of bad news when trust in elections is already low, but the public needs accurate information about election security. Whether our findings ultimately strengthen or weaken public trust will depend on how responsible officials respond.

The most effective remedy for the problems we found and others like them is to rely less on BMDs. The risk of attack is much lower when only a small fraction of voters use BMDs, as in most states, than when all in-person voters are forced to use them, as in Georgia. Where BMDs must be used, the risk of an undetected attack can be reduced by avoiding using barcodes to count votes. Officials can configure the ICX to print traditional-style ballots that do not use QR codes. This has the virtue of forcing an attacker to make changes that are (at least in principle) visible to voters. States should also implement rigorous risk-limiting audits of every major contest, which [the National Academies has called on all states to do](#) by 2028.

Our findings in Georgia demonstrate that elections face ongoing security risks that call for continued vigilance from policymakers, technologists, and the public. In light of these risks, the best way for officials to uphold voter confidence is to further improve security, not to deny that problems exist.

---

FILED UNDER: [PRIVACY & SECURITY, VOTING](#) TAGGED WITH: [SECURITY, VOTING](#)