

# Dominion Ballot Marking Device Security Flaws



June 26, 2023

Halderman ICX BMD Security Analysis

Garland Favorito

*Security Analysis of Georgia's Image  
Cast X Ballot Marking Devices*

*Prof. Alex Halderman*

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

REDACTED VERSION

**Security Analysis of Georgia's  
ImageCast X Ballot Marking Devices**

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

Prof. J. Alex Halderman, Ph.D.

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

July 1, 2021



# Georgia Unverifiable Voting History

**2002:** Georgia bought Diebold paperless voting system and became first state to implement such a system statewide over many written objections (including mine)

**2009:** Georgia Supreme Court denies VoterGA claims stating the voter bears responsibility for unequal voting systems

**2019:** U.S. District Court found Diebold DRE voting system unconstitutional, banned it for 2020 and future (*Curling v. Raffensperger*)

**2020:** U.S. District Court found new QR coded Dominion voting system violates two Georgia statutes unconstitutional, banned it for 2020 and future (*Curling v. Raffensperger*)



# Who is Alex Halderman?

- ❖ University of Michigan Computer Science and Engineering Professor
- ❖ Expert witness in *Curling v. Raffensperger* who had physical access to evaluate Georgia's Dominion voting system
- ❖ As a student at Princeton he participated in Dr. Ed Felten's team that hacked the Diebold voting system before the Committee on House Administration in 2006

<https://youtu.be/sVzMmpPgnSg>



# Security Analysis of GA's Dominion ICX BMD's

- ❖ Analysis was sealed for 2 years but available to CISA, Dominion & parties in *Curling v. Raffensperger*
- ❖ Goes far beyond CISA report that identified 9 flaws after this analysis was sealed
- ❖ Provides academic research & testing that confirms our key claims of the last 3 years and makes many more vulnerability assertions
- ❖ Analysis limited to Dominion ICX Ballot Marking Device (BMD)
- ❖ Analysis could have been equally as devastating for ICP scanner tabulators



# Security Analysis By Section

- ❖ Principal Findings
  - ❖ Encryption and Encoding
  - ❖ QR Codes
  - ❖ Access Cards
  - ❖ Logic & Accuracy Testing
  - ❖ Malware Creation
  - ❖ Spreading Malware
  - ❖ Audit Log Manipulation
  - ❖ Unsafe, Extraneous Applications
  - ❖ ICP Scanner Vulnerabilities (out of scope)
- ❖ Main Conclusions and **Bottom Line**

# Halderman's Principal Findings Page 4-5

"I show that the ICX suffers from critical vulnerabilities that can be exploited to subvert all of its security mechanisms,..."

"I demonstrate that these vulnerabilities provide multiple routes by which attackers can install malicious software on Georgia's BMDs, either with temporary physical access or remotely from election management systems (EMSs)."

"I explain how such malware can alter voters' votes while subverting all of the procedural protections practiced by the State..."



# Halderman's Principal Findings QR codes/voter cards, Page 4-5

“Attackers can alter the QR codes on printed ballots to modify voters’ selections. (Section 7).”

“Attackers can forge or manipulate the smart cards that the ICX uses to authenticate technicians, poll workers, and voters. (Section 6).”

“It is very likely that there are other, equally critical flaws in the ICX that are yet to be discovered...but attackers would only have to find one.”

# Halderman's Principal Findings – GA software update Page 4-5

“The software update that Georgia installed in October 2020 left Georgia’s BMDs in a state where anyone can install malware with only brief physical access to the machines.”

“I show that this problem can potentially be exploited in the polling place even by non-technical voters (Section 8).”

-



# Halderman's Principal Findings – Mass distribution Page 4-5

“I demonstrate that attackers can execute arbitrary code with root (supervisory) privileges by altering the election definition file that county workers copy to every BMD before each election. “

“Attackers could exploit this to spread malware to all BMDs across a county or the entire state (Section 9).”

-

# Halderman on Encryption and Encoding Page 20-21

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

“Although the QR codes are not encrypted, they use a data format is incompatible with most off-the-shelf barcode reader software.”

-

# Haldeman on QR Codes Page 20-21

“...there is no mechanism for detecting duplicate QR codes...”

“the codes do not contain a serial number or other unique identifier, so, for a given ballot design, all QR codes that contain identical votes are indistinguishable”

“In a “replay” attack, attackers observe genuine printed ballots and save copies of QR codes with votes they favor. They then alter ballots with votes they disfavor by replacing the QR codes with the ones they have saved. “

“An attacker also could choose to change only the QR code or both the QR code and the human-readable text.”

# Halderman on ICX Access Cards Page 26-27

“Weaknesses in the ICX authentication protocol allow an attacker to read and forge Voter, Technician, and Poll Worker cards.”

“ICX Technician Cards are not restricted to a particular election or a particular jurisdiction. Consequently, the forged Technician Cards I created will work in any ICX across the State of Georgia, and likely in any other jurisdiction that uses a compatible version of the machine.”

After forging a Technician Card, an attacker with physical access to a BMD can exit the ICX application and access the underlying Android operating system. With this access, the attacker can arbitrarily change the BMD’s configuration, alter audit logs, or install malicious software.”

“Georgia’s LAT procedures (Exhibit B) involve only minimal testing of the ICXs. Only a single test ballot per ICX is required to be printed. To avoid detection, the demonstration malware simply tracks how many ballots have been printed since the machine was turned on and skips cheating on the first  $n$  ballots...”

- 

“For example, malware could be programmed to only cheat on the day of the election, or only during specific hours on that day.”

“No practical method of pre-election or parallel testing can rule out malware-based fraud.”

-



# Halderman on Malware Creation Page 32-40

“The ICX fails to adequately restrict the kinds of devices that can be attached to its USB ports, including the externally exposed USB cable that connects to the printer.”

“Dominion could have used digital signatures to limit installation of apps to those signed by the company,... However, my tests show that the ICX does not verify the identity of the signing party.”

“I conclude that malware is easier to create for the ICX system than it was for Georgia’s old DRE system.”

•



# Halderman on Spreading Malware Page 48

“An attacker who infiltrates a county’s EMS can modify the county’s *ICX.dat* file before it is copied to USB drives, and thereby spread malware to all BMDs in the county.”

“At Dominion, an attacker who infiltrates the facility where Dominion prepares Election Projects could modify the election definitions distributed to all Georgia counties, and thereby spread malware to every ICX used in Georgia.”

# Halderman on Audit Log Manipulation Page 54

“Weaknesses in the ICX allow attackers to easily gain root privileges, which lets them bypass all file system access controls. Consequently, attackers can arbitrarily edit or erase the audit logs, and they can change the protective counters to any value they choose.”

“An attacker with physical access to the BMD can manipulate the logs and counters via several routes.”

“I confirmed that this technique can successfully ‘roll back’ the lifetime counter to a previous value, allowing the attacker to conceal having printed arbitrarily many ballots.”

# Unsafe Extraneous Applications — Page 4-5

“The ICX contains numerous unnecessary Android applications, including a Terminal Emulator that provides a ‘root shell’ (a supervisory command interface that overrides access controls).”

“An attacker can alter the BMD’s audit logs simply by opening them in the on-screen Text Editor application. (Section 10)”

-

## Halderman on Scanners (out of scope) Page 57

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

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

“...the message authentication codes in the QR codes do not allow the scanners to distinguish between original and duplicate ballots, so, absent a check on the physical paper stock, the scanners cannot detect photocopied ballots.”

# Halderman's Main Conclusions Page 6-7

“The ICX BMDs are not sufficiently secured against technical compromise to withstand vote-altering attacks by bad actors who are likely to attack future elections in Georgia.”

“Despite the addition of a paper trail, ICX malware can still change individual votes and most election outcomes without detection. Election results are determined from ballot QR codes, which malware can modify, yet voters cannot check that the QR codes match their intent, nor does the state compare them to the human-readable ballot text.”

# Halderman's Main Conclusions Page 6-7

“Using vulnerable ICX BMDs for all in-person voters, as Georgia does, greatly magnifies the security risks compared to jurisdictions that use hand-marked paper ballots but provide BMDs to voter upon request. “

“My technical findings leave Georgia voters with greatly diminished grounds to be confident that the votes they cast on the ICX BMD are secured, that their votes will be counted correctly, or that any future elections conducted using Georgia’s universal-BMD system will be reasonably secure from attack and produce the correct results. “



## Halderman's Bottom Line Page 6-7

“The critical vulnerabilities in the ICX—and the wide variety of lesser but still serious security issues—indicate that it was developed without sufficient attention to security during design, software engineering, and testing.”

“In my view, it would be extremely difficult to retrofit security into a system that was not initially produced with such a process.”

“No grand conspiracies would be necessary to commit large-scale fraud, but rather only moderate technical skills of the kind that attackers who are likely to target Georgia's elections already possess.”



# Raffensperger Letter



Georgia  
Secretary of State  
Brad Raffensperger

 SOS Office ▾  Business ▾  Charities ▾

## Setting the Election Security Record Straight

[Home](#) > [News & Announcements](#) > Setting the Election Security Record Straight

**June 20th, 2023**

Dear Members of the General Assembly,

Georgia's election system is secure. It's been battle-tested through two general elections, subjected to repeated audits and intense public scrutiny, and come through with flying colors. Georgia's election officials are proceeding judiciously and responsibly to ensure that our elections are secure, accurate and accessible to the voters. Every single piece of voting equipment across Georgia will undergo security health checks ahead of the 2024 presidential elections, including verification no software has been tampered with.

The current proposed software upgrade has never been deployed for a major election anywhere in the nation. There are pilot tests of the upgrade that will take place in some local jurisdictions in Ohio, and Georgia will test it in some municipal elections this fall. In an initial evaluation by our election officials, the upgraded software was found to be incompatible with our poll pads. Discovering that problem during an election would have caused chaos. Discovering it ahead of time allows us to develop a patch that addresses the issue without risking any election or public trust in the results.

©2023 Voters Organized for Trusted Election Results in Georgia Est. 2006 – VoterGA.org



# Mitre Report

- ❖ Unsigned
- ❖ Funded by Dominion Voting Systems
- ❖ Produced without access to voting system
- ❖ Based on premise that perfect security controls exist

MITRE

MP220250  
MITRE PRODUCT

**Independent Technical  
Review: *Security Analysis of  
Georgia's ImageCast X Ballot  
Marking Devices***

**July 2022**

The analyses, views, opinions, and findings contained in this report are those of The MITRE Corporation only and should not be construed as those of any other person, organization, or company.

©2022 The MITRE Corporation.  
All rights reserved.

McLean, VA



# Mitre Expert Rebuttal

29 Cybersecurity experts and computer science academic wrote to Mitre CEO seeking retraction of “ridiculous” report

Sincerely,<sup>7</sup>

Josh Aas, Executive Director, Internet Security Research Group

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

Andrew W. Appel, Eugene Higgins Professor of Computer Science, Princeton University

Duncan A. Buell, Chair Emeritus, NCR Chair in Computer Science and Engineering, University of South Carolina, Columbia

Richard DeMillo, Professor and Charlotte B and Roger C Warren Chair in Computing, Georgia Tech, Atlanta GA

Zakir Durumeric, Assistant Professor of Computer Science, Stanford University

Aleksander Essex, Associate Professor of Software Engineering, Western University, Canada

Michael J. Fischer, Professor of Computer Science, Yale University

Robert Graham, cybersecurity expert

Matthew D. Green, Associate Professor of Computer Science, Johns Hopkins University

Harri Hursti, independent security researcher, co-founder Voting Village @ DEF CON

David Jefferson, Computer Scientist, Lawrence Livermore National Laboratory (retired)

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

Joseph Kiriir, Principal Scientist - Galois & CEO and Chief Scientist - Free & Fair

Patrick McDaniel, Tsun-Ming Shih Professor of Computer Sciences, University of Wisconsin-Madison

Prateek Mittal, Professor, Princeton University, Interim Director, Center for Information Technology Policy (CITP)

Olivier Pereira, Professor, UCLouvain

Ronald L. Rivest, Institute Professor, Massachusetts Institute of Technology

Peter Y A Ryan, University of Luxembourg

Peter B. Rønne, Chercheur, CNRS, LORIA, France

Bruce Schneier, security technologist and Lecturer, Harvard Kennedy School

E. John Sebes, Chief Technology Officer, OSET Institute

Barbara Simons, Computer Scientist, IBM Research (retired)

Kevin Skoglund, Chief Technologist, Citizens for Better Elections

Eugene H. Spafford, Professor, Executive Director Emeritus, CERIAS, Purdue University

Michael Alan Specter, PhD, Security Researcher

Philip B. Stark, Distinguished Professor of Statistics, University of California, Berkeley

Vanessa Teague, CEO, Thinking Cybersecurity Pty Ltd and Associate Professor (Adj.), The Australian National University

Poorvi L. Vora, Professor of Computer Science, The George Washington University

<sup>7</sup> Affiliations are listed for identification purposes only and do not indicate endorsement by the institutions mentioned therein.





# VoterGA Letter

- ❖ Sent to all legislators
- ❖ Sent to all county election officials
- ❖ Included Expert rebuttal of Mitre Report
- ❖ Included VoterGA Fact Check of SOS letter



June 22, 2023

Dear Georgia Legislators,

I am writing in response to Secretary of State Brad Raffensperger's public [letter](#) dated June 20, 2023, that was sent to you on Tuesday. The letter from the Secretary of State entitled "Setting the Election Integrity Record Straight" actually does the opposite. I have attached a [VoterGA Fact Check](#) explaining why Secretary Raffensperger's letter to you contained 15 false or misleading statements. If you would like more supporting detail for our Fact Check please contact me.

The Secretary's letter attempts to convince Georgia's public officials that Georgia elections are secure. Ironically, Secretary Raffensperger is preventing anyone from proving elections are secure by fighting to keep ballots sealed after every election. Any reasonably intelligent person should be able to see this as the ultimate hypocrisy. No one can honestly claim security in their elections while continuously fighting to prevent transparency for those elections.

The MITRE report mentioned in the letter and the call yesterday was funded by the Dominion voting system vendor and produced without access to any of Georgia's voting equipment. Its non-standard approach to security analysis assumes perfect physical security procedures exist and it has already been [discredited](#) by 29 experts.

By contrast, the [Halderman Security Analysis](#) mentioned in the call was produced with access to the Dominion voting system as part of the *Curling v. Raffensperger* case. It is important to remember this case was initiated in 2017 after the Center for Elections Center (CES) failed for six months to mitigate a server breach identified by a Bastille Threat Research Team member who reported it to them. Days after the case was filed, then CES Director Michael Barnes allowed the election servers to be wiped clean without properly mitigating the breach. Mr. Barnes was part of the call yesterday. Our [VoterGA study](#) documents the breach and that destruction of election data.

In 2021, SB202 took a great first step in transparency by making public the digital ballot images used to produce cast vote records and tabulate results. However, we found they are too low a resolution to detect counterfeits such as those senior pol managers identified during a 2020 hand count in one county. In that same county we further [determined](#) that the ballot images were electronically altered before 2020 results were certified. That is why making only ballot images public is inadequate to ensure the security of Georgia elections.

To prove elections are secure, physical ballots must be unsealed and subject to Open Records Requests immediately after an election is certified. These public records should be available for inspection in the custody of election officials and for high resolution copying at the requestor's expense independently of the voting equipment. They can then be used to verify election results, detect counterfeits, facilitate election security and restore voter trust in Georgia elections.

Bills already have been introduced this session to accomplish these objectives. Please help us achieve election transparency this session by passing SB122 or HB426.

Sincerely,  
Garland Favorito  
Co-founder  
404 664-4044 CL



# Raffensperger Fact Check [voterga.org/Studies](https://voterga.org/Studies) tab

Raffensperger letter contained:

- ❖ 5 False Statements
- ❖ 6 Mostly False Statements
- ❖ 5 “Pants on Fire” Lies

VOTERGA.ORG FACT CHECK		
June 20, 2023 GA SOS Brad Raffensperger		
False Statements - 4 Mostly False - 6 “Pants on Fire” - 5		
Rating	<a href="#">“Setting The Election Record Straight”</a>	ACTUAL VOTERGA FACTS
	“Georgia’s election system is secure”	Ha! <a href="#">Numerous experts</a> have provided court testimony and letters to government officials confirming it is not secure
	“...it has been subject to repeated audits...”	The voting system had only one audit every 2 years <a href="#">by law</a>
	“... and [the system has] come through with flying <a href="#">colors</a> .”	The voting system <a href="#">declared wrong winners</a> for DeKalb District 2 Commission which was the only 2022 primary race that was fully audited
	“The ‘critics of Georgia’s election security’ ... are from one of only two groups: election-denying conspiracy theorists or litigants...”	Critics include <a href="#">cybersecurity experts and science professors</a> throughout the country. The demeaning terms used by the author are intentionally designed to deceive the reader
	“These two groups make ever-shifting but always baseless assertions that Georgia’s election system is at risk ...”	Assertions were confirmed by <a href="#">Senate Judiciary</a> and House Government Affairs Committees, county election boards and <a href="#">Governor Kemp’s 36-point study</a> for the State Election Board
	“We ... conducted a risk-limiting audit and a full hand recount of every ballot in Georgia to prove that our results were accurate....”	<a href="#">VoterGA determined</a> the Fulton Co. full hand recount had a 60% batch error rate, falsified tally sheets, 300+ duplicate scanned ballots and 4,000+ duplicate reported ballots
	“The 2022 elections saw ... virtually zero complaints about the process -or the results”	In 2022, a candidate was <a href="#">found to have gotten no votes</a> in the precinct where she and her husband lived and voted
	“That system, proven and tested, is the system we have in place today for Georgia elections.”	The system has been tested but has not been proven to always count accurately
	“We have layers of security protocols and procedures to physically protect ballots, the system, the software, and the results.”	Security protocols and procedures do not include ballot inspections and are inadequate to protect voters against counterfeit ballots and incorrect results
	“We have tests and audits to verify results.”	Tests cannot verify results because they are run before the results are produced
	“It identified risks that are theoretical and imaginary.”	The <a href="#">Halderman Security Analysis</a> identified risks that are real, not imaginary
	“The MITRE report ... points out that the vulnerabilities described by Halderman as operationally infeasible.”	<a href="#">The MITRE report</a> was funded by Dominion, produced without access to a voting system and assumes perfect procedural defenses, <a href="#">called “ridiculous” by 29 experts</a>
	“One attack was technically scalable but also...infeasible due to access controls in place...”	Counties have no access controls to detect malware attacks when received in election definition files as the <a href="#">Halderman Security Analysis</a> points out
	“Is it possible for a team of bad actors to break into Georgia’s 2700 voting precincts, install malware...It’s more likely that I could win the lottery without buying a ticket.”	<a href="#">Halderman explains</a> no break in is needed when the state system can currently distribute election definition malware to all counties. That malware can then spread to each scanner and touchscreen without detection
	“I believe that legislative consideration for increasing the penalties ... would demonstrate to the people of Georgia that we take their elections seriously.”	Making ballots public record to detect counterfeits and verify election results would tell the people of Georgia that they take elections seriously



# How to Secure 2024 Elections?

**VOTERGA**.ORG

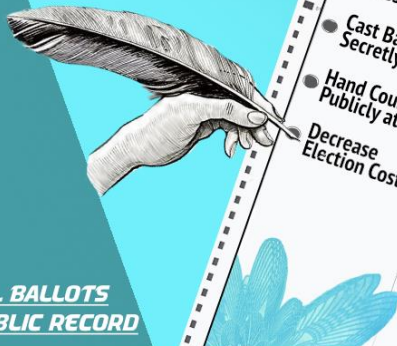
## UNPLUG GEORGIA

with

### SECURE PAPER BALLOTS

HAND MARKED and HAND COUNTED

...at the polls



**ALL BALLOTS PUBLIC RECORD**

*Confidence in elections. Real Ballot under UV Light*

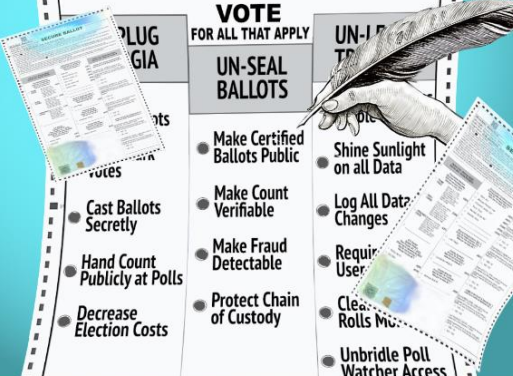
*Voters Organized for Trusted Election Results Visit: VoterGa.org*

**VOTERGA**.ORG

## UNSEAL BALLOTS

If ballots are public we can...

### VERIFY ELECTION RESULTS & DETECT COUNTERFEITS




**Georgia Legislators Must Act Now!!!**

**VOTERGA**.ORG

## UNLEASH TRUST

with

### TRANSPARENT ELECTION PROCESSES



**IT'S TIME FOR SOME SUNLIGHT!**

*Voters Organized for Trusted Election Results Visit: VoterGa.org*



# Connect with us Online



[VoterGA.org/Donate](https://VoterGA.org/Donate) Tab


All donations are tax deductible

[Donate Now](#)

@VoterGA

#VoterGA

 Facebook

 YouTube

 Twitter

 Rumble

 Gab

 Bit Chute

 Telegram

 Brighteon

 Gettr

 Instagram

 Parler

 LinkedIn