SHARE:

Join Our Email List

View as Webpage

Coalition for Good Governance

Halderman Report on Georgia's Voting System Vulnerabilities Unsealed by Federal Court

Voting system vulnerabilities confirmed by Department of Homeland Security; Georgia Secretary of State signals no plans to mitigate the risks.

Atlanta, GA (June 14, 2023) – The U.S. District Court for the Northern District of Georgia has unsealed Prof. J. Alex Halderman's **Security Analysis of Georgia's ImageCast X Ballot Marking Devices**, a 96-page report ("Halderman Report") that describes numerous security gaps affecting Dominion touchscreen voting equipment used in Georgia and other states.[1] The report identifies system vulnerabilities that require prompt effective mitigations according to the Department of Homeland Security prior to the 2024 election cycle. However, the Georgia Secretary of State's office has stated it will not adopt software updates to address the demonstrated security risks until at least 2025. Neither the Secretary of State nor the State Election Board have announced plans to enhance voting system security or implement any mitigations to the reported and proven system security flaws.

"Coalition for Good Governance ("CGG"), the organizational plaintiff in the long-running voting rights lawsuit for which Dr. Halderman's expert report was prepared for the Curling Plaintiffs, is pleased to provide this essential report to the press, government officials and the public, along with companion information from renown experts. The irrefutable scientific facts compel immediate action by Georgia officials to protect the 2024 elections." said Marilyn Marks, its Executive Director. Such companion information is linked below, with supplemental information attached.

After receiving access to the touchscreen ICX ballot marking device (BMD) through a court order, Prof. Halderman and his fellow researcher, Prof. Drew Springall assessed the BMD system's susceptibility to cyberattacks, and found and validated several major vulnerabilities. The resulting report was filed with the court

in July of 2021 and promptly sealed. The Georgia Secretary of State and State Election Board were authorized to review the report. With court approval, the sealed report was also submitted to the Department of Homeland Security's Cybersecurity and Infrastructure Agency ("CISA"), which replicated and verified Profs. Halderman and Springall's findings.

CISA recommended the risks "should be mitigated as soon as possible," but Georgia state officials have not taken any action to adopt the recommended mitigations. In fact, counsel for Georgia Secretary Raffensperger recently advised the court that the state has no plans to address the security vulnerabilities identified by Halderman and CISA until 2025, after the presidential election year.

Delaying the security patches until 2025 is "worse than doing nothing," warned Prof. Halderman, "since it puts world-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 security risks identified are further elevated by the fact that Georgia's voting system software was unlawfully copied and distributed by operatives associated with the Trump campaign. Partisan operatives have covertly shared copies of the software with an unknown number of individuals and entities.

The previously sealed technical report is supplemented by Dr. Halderman's reader-friendly overview which explains how would-be attackers can plant vote-stealing or election disrupting malware. This overview offers a big picture view of the "real world" implications of the long-awaited detailed technical report of the touchscreen system vulnerabilities. It also explains how the opportunity to plant such malware through usb sticks is available to thousands of election staff members, temporary workers loading balloting software, testing, delivering and setting up voting machines in polling places, polling place maintenance staff, poll workers, staff working with the county central server, and voters themselves. In short, physical access to the voting touchscreens (ICX), and sometimes the office election system servers (EMS), is available to adversaries and can be scaled for widespread impact, even when physical access is limited to a few machines or servers.

"I hope the Halderman report puts an end to Secretary Raffensperger's fairy tale that attacks are impossible because the machines are not connected to the Internet," said Georgia Tech Professor and founder of the School of Cybersecurity and Privacy Richard DeMillo. "It's especially ironic that, according to a recent AJC article, Governor Kemp, the former Secretary of State, had to travel to Israel to see 'haunting examples of how easily a computer or smartphone can be hacked — even if they're not connected to the Internet.' " DeMillo added.

# # #

Supplemental Information on Georgia's Voting System Security and the Halderman Report

Unauthorized access to Georgia's election systems occurred in Coffee County; new evidence indicates unlawful access may extend to Treutlen County.

Key Document-- The previously sealed technical report is supplemented by **Dr. Halderman's reader-friendly overview** which explains how would-be attackers can plant vote-stealing or election disrupting malware.

In January 2021, operatives associated with the Trump campaign were given access to all the components of the Georgia voting system over several days. The operatives copied the voting system software, uploaded it to a private file sharing site, and covertly distributed it to other individuals and entities engaged in efforts to overturn the 2020 presidential election. The alarming facts of the Coffee County breaches and spread of the state's current voting software to many more rogue actors are explained in detail by CGG's expert Kevin Skoglund in his comprehensive expert report. Professor Halderman also filed an additional expert report focused on the cybersecurity dangers of the statewide breach. Both expert reports are written with plain language explanations of how the system was compromised and the implications for future elections.

It was recently reported that the Georgia SOS office seized the election server in Treutlen County in response to evidence that indicates that, Misty Hampton, the election supervisor who allowed the unlawful access to Coffee County voting systems, subsequently was hired by Treutlen County after she was fired from Coffee. CGG obtained information that Hampton was engaged (without documentation) to program and test the Treutlen County voting system in the spring and summer of 2021. Though these **f**acts first surfaced in discovery in November 2022, Secretary Raffensperger and the State Election Board did not investigate how Ms. Hampton was permitted to access the voting system in Treutlen County, until CGG urged them to do so in March, 2023. The Secretary of State's office seized the Treutlen server in April, 2023.

Cybersecurity Experts Urged the Court to Unseal the Halderman Report

While it may seem counterintuitive to release the details of how the voting system can be exploited, cybersecurity experts across the nation strongly agree that responsibly publicly disclosing the details of the vulnerabilities serves to permit officials to understand why they must take action to protect upcoming elections, and what they must do. Neither vendors, such as Dominion in this case, nor the U.S. Election Assistance Commission are motivated to disclose the weaknesses in their own previous work that permitted these security weaknesses to be certified and used in public elections. Numerous experts wrote reports to the court to urge the release of the Halderman Report to better secure the upcoming elections. Experts agree that bad actors are known to possess Georgia's software and must be presumed to have researched the vulnerabilities at least to the same extent that Professors Halderman and Springall did. They acknowledge that their 12 man-weeks of work, if extended, would likely have unearthed more vulnerabilities. With the widespread rogue distribution of the Georgia software through the Coffee County perpetrators, now for 30 months, it is only reasonable to expect that many more vulnerabilities have been discovered along with clever methods of making attacks undetectable.

Experts Call for Retraction of Misleading Dominion-Sponsored MITRE Report

In response to the Halderman Report, Dominion hired MITRE to provide a response report, then shared Halderman's sealed report, without Court authorization. MITRE was not given access to the software or equipment to perform any actual tests, or

replicate the work performed by Halderman and Springall. The resulting report predictably downplays the severity of security flaws in the Dominion system. MITRE's response report is premised on the demonstrably false core assumption that physical security of the system is sufficient to prevent access by would-be attackers. The unsigned report, dated July 2022, does not contemplate the unauthorized access that occurred in Coffee County, even though Dominion and the Secretary of State were aware of the January 7, 2021 breach long before the report's issuance and the press was reporting credible breach allegations of the breach in May and June 2022.

In fact, according to a memo from a Coffee County election official, (improperly withheld from disclosure in litigation by the Secretary of State and Coffee County officials), the Secretary of State had been apprised of serious physical security lapses in Coffee County in August of 2021. The alarming memo undercuts MITRE's and Secretary Raffensperger's July 2022 assurances that physical security is routine and adequate. Spurious claims of effective physical security of voting system components and the software loaded on them are debunked by real world circumstances, such as this recent CNN report of a Dominion ICX touchscreen purchased on eBay.

In light of the deeply flawed assumptions underpinning MITRE's report, experts are calling for MITRE to retract it. Professor Richard DeMillo, founder of Georgia Tech's School of Cybersecurity and Privacy said, "The unsigned MITRE report, which conveniently skipped examining the system, ridiculously downplays the danger of compromise by blindly trusting Dominion and Georgia election officials. Their naive belief in the difficulty of accessing the system software is unfounded. The news of unauthorized access in Coffee County alone should be sufficient to discredit MITRE's report. It's high time they retract their misguided effort."

"MITRE says it assumed there would be 'strict and effective controlled access to Dominion election hardware and software,' but we now know that unauthorized individuals have already breached those access controls. MITRE's risk analysis and conclusions are therefore invalidated. They should do the right thing and retract their report and its conclusions," said Dr. Duncan Buell, Emeritus NCR Chair, Computer Science, University of South Carolina.

"Just based on the Executive Summary of the MITRE report alone, it seems that the anonymous authors fail to understand the full range of the realistic threats to elections. They apparently assume the physical security of Georgia voting systems is sufficient to preclude any feasible attack, whereas the reported breach in Coffee County had publicly demonstrated it was very real danger months before the MITRE report was prepared. They also seem not to consider the possibilities of insider attacks, or of malware introduced centrally and then distributed to some or all voting machine in the county or state. MITRE should either withdraw this report or else substantially amend it in the light of the facts on the ground," said Dr. David Jefferson, computer scientist recently retired from Lawrence Livermore National Laboratory.

MITRE suggests that if the vulnerabilities were exploited, they would be detected, but to do this MITRE grossly misrepresents Georgia's law and practices governing vote counting and Georgia audits. Georgia's post-election audits are historically ineffective, and the 2023 General Assembly further gutted the already hapless audit law. Further, the unnamed authors asserted that the QR Code vote was not the "authoritative vote" in Georgia, which is plainly incorrect. The hackable QR Code

vote is ***the*** vote counted in original counts and recounts, except in the rarest of exceptions.

CGG anticipates a chorus of expert computer scientists' calls for MITRE to retract the misleading report to avoid confusion of election administrators faced with these urgent decisions.

Georgia SOS Recently Announced System "Health Checks"

Georgia's touchscreen voting system, with its inherent proven security flaws, and compromised by the 2021 breaches emanating from Coffee County, is slated for certain "testing" according to a May 19, 2023 press release issued by Secretary of State Raffensperger, calling the testing a "health check" of the system.

"Using imprecise terms like "health check" to describe highly technical cybersecurity concepts might lead people to believe that adequate steps were being taken to secure our election systems when the opposite is true. There is no agreed-upon definition of a security 'health check,' although it is most often applied to deep analysis to expose vulnerabilities, not verifying hash values to determine whether the software has been changed, as the Secretary of State claims. The way that Dominion calculates and displays those values was identified in a public CISA advisory as a vulnerability (CVE-2022-1740, often called a mutable attestation vulnerability) that can be easily exploited to disguise malware on a device and therefore fool the 'health check,'" said DeMillo.

"Georgia has a long history of poor management of election security. In the last two decades state officials have made bad selections of voting systems and installed them statewide. Over that time, they have consistently ignored most of the advice of national experts regarding the election integrity and cybersecurity. Now they are refusing to acknowledge the severity of the vulnerabilities discovered by Prof. Alex Halderman, and are failing to properly investigate and deal with the massive Coffee County software breach that also endangers election security in every county in the state (since they all run the same software).

"The so-called "health check" that officials are planning will simply attempt to verify hash values to check that version 5.5A of the Democracy Suite software is intact. It will do very little to mitigate the threats to future elections since that version has severe security vulnerabilities and is also the very version that was reportedly stolen in Coffee County. The most important action Georgia officials can take to protect the 2024 elections is to switch to hand-marked paper ballots and abandon the ballot marking machines (except for disabled voters). That would go a long way toward enabling real risk limiting audits (RLAs) and securing Georgia's elections in the future," said Dr. David Jefferson,

Georgia Audits are an Ineffective Check on the BMD Touchscreen Voting System

Dr. Philip Stark, the nation's foremost expert in post-election auditing and the inventor of Risk-Limiting Audits for elections, explained, "Georgia's audits cannot detect BMD hacking, misconfiguration, or misbehavior, and cannot provide evidence that election outcomes are correct—i.e., that the reported winners really won. Georgia needs to abandon universal-use BMDs and primarily use hand-marked paper ballots, with exceptions for accessibility; to substantially strengthen its

canvass, including physical accounting and chain of custody requirements for ballots, memory cards, and other election materials; and to enforce those requirements. Only then will it be possible for a properly designed and executed audit to provide evidence that outcomes are correct. Georgia's 2020 audit and machine recount did not even notice that many votes had been counted twice. Since then, Georgia has weakened its audit requirements, which were inadequate in the first place."

CGG: Commonsense Solutions Await Simple Action by Georgia Officials

Georgia officials can mitigate these risks with the simple decision to deploy the emergency back-up balloting procedures in the current Election Code. Such backup balloting procedures are routinely used when BMD touchscreen units are inoperable. Ballots are marked coloring in ovals with pens, and ballots are cast and tabulated in the current scanners. Supplemental audits should be mandated.

"Faced with irrefutable damning evidence of the massive breach, state election officials shockingly simply chose silence as their 2022 mid-terms security strategy, undertaking no mitigations, emergency measures, incident investigation, or even security protocol guidance to the counties," said Marilyn Marks, CGG's Executive Director. "The state's continued see, hear, speak no evil strategy has continued with the 2024 elections looming. We were shocked to learn in May that the state plans none of the urgently needed mitigations verified by CISA, and reported by Dr. Halderman. Secretary Raffensperger has concluded that the touchscreen equipment mitigations are complex and will require tens of thousands of technician hours to deploy, so he will postpone addressing the needed patches and upgrades until after 2024's presidential election.

Voting system computer scientists and cybersecurity experts across the nation agree that 1) delaying the Dominion software update until 2025 is an unnecessary high risk decision, and 2) the announced "health checks" are wholly inadequate responses to a security crisis facing the 2024 elections."

CGG has recently petitioned the State Election Board to adopt Election Code provisions which would 1) define system security incidents and vulnerabilities, 2) require prompt mandatory reporting of security incidents and detected vulnerabilities, and 3) require back-up balloting as a mitigation until security incidents are determined to be have been otherwise mitigated. These commonsense requirements should be immediately adopted as election rules. They are basic protocols that even modest-size businesses and organizations have, but are not covered in Georgia's Election Code. Numerous other organizations and individuals have weighed in to support CGG's rule-making petition. Should the State Election Board adopt the proposed rules, the 2021 breaches of the voting system would likely be mitigated with the use of hand marked paper ballots (Georgia's back up balloting system) in 2024. A hearing on the proposed rules will be held at the upcoming June 21 meeting.

Basic Voting System Security Prevents Election Subversion

Bruce Brown, attorney representing CGG and four voter plaintiffs in the Curling litigation summarized this important case development saying, "The court's unsealing of the essential Halderman Report marks an important new chapter in this voting rights case. The Report provides compelling evidence that officials must adopt

trustworthy hand marked ballots as a basic constitutional requirement to avoid the subversion of our democratic elections. Adopting commonsense measures such as hand marked ballots, scanned tabulation, and audits of outcomes ensures that the outcomes will be correct and that the public will have confidence in the integrity of the system.

The state constitutional right to an absolutely secret ballot for every voter is essential to vigorously protect when partisan extremism is in play. With their large bright displays of voters' candidate selections, Dominion touchscreen ICX units permit the public to see how voters are voting, violating Georgia's secret ballot protections. Voter suppression and election subversion become the natural results of violations of our long-standing rights to a secret ballot. Conducting Georgia's 2024 elections with back up balloting procedure using hand marked ballots counted by precinct scanners vindicates every voters' right to vote their conscience in secret without fear of reprisal."

The Curling case is in its sixth year in federal court, having achieved a landmark voting rights victory in 2019 in its first phase by obtaining a court order ridding the state of paperless Diebold touchscreen voting machines. The second (BMD) stage of the case is now awaiting the resolution of the State's Motion for Summary Judgment before a trial date is set. The Curling Plaintiffs' brief in response to the motion provides an overview of the election security issues at the core of the case and the status of the case.

Coalition for Good Governance is a nonpartisan, nonprofit organization focused on fair and transparent elections.

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

[1] The report does not allege or support any claims of election fraud in the 2020 election.