September 8, 2022

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

Dear Chair Duffey and Members of the State Elections Board:

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

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

The immediate concern

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

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

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

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

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

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

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

In 2020 Georgia finally abandoned its insecure, paperless, touchscreen Diebold voting machines. Ignoring recommendations from election security experts[5] and public preference,[6] the Secretary of State successfully pushed the State legislature to approve a universal use BMD touchscreen voting system. The BMD system has put Georgia's elections at a higher risk for tampering, disruption, or allegations of

---

[3] Tierney Sneed, "Judge sanctions pro-Trump lawyers who brought 'frivolous' lawsuits," *CNN,* August 26, 2022. *Available at: https://www.cnn.com/2021/08/25/politics/judge-sanctions-powell-wood-kraken-lawsuits/index.html*

[4] "Report of the Auditability Working Group," National Institute of Standards and Technology, 2010. *Available at: https://www.nist.gov/document/auditabilityreportxml-7htm*

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

[10] Mark Neisse, "Handling of Georgia election breach investigation questioned," Atlanta Journal Constitution, September 4, 2022. Available at: Questions surround handling of election breach investigation in South Georgia county (ajc.com)

[11] Emma Hurt, "What's going on with Coffee County?", *Axios,* September 7, 2022. Available at: 2020 election investigation puts a spotlight on Coffee County, GA - Axios Atlanta

[12] See *supra* note 9.

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

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

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

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

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

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

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

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

Yours truly,

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

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

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

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

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

Susan Greenhalgh
Senior Advisor for Election Security
Free Speech For People

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

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

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

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

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

Kevin Skoglund
President and Chief Technologist
Citizens for Better Elections*

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

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