November 13, 2024

The Honorable Kamala Harris
The White House
Office of the Vice President
1600 Pennsylvania Avenue, N.W.
Washington, DC 20500

Dear Vice President Harris,

We write to alert you to serious election security breaches that have threatened the security and integrity of the 2024 elections, and to identify ways to ensure that the will of the voters is reflected and that voters should have confidence in the result. The most effective manner of doing so is through targeted recounts requested by the candidate. In the light of the breaches we ask that you formally request hand recounts in at least the states of Michigan, Nevada, Wisconsin, and Pennsylvania. We have no evidence that the outcomes of the elections in those states were actually compromised as a result of the security breaches, and we are not suggesting that they were. But binding risk-limiting audits (RLAs) or hand recounts should be routine for all elections, especially when the stakes are high and the results are close. We believe that, under the current circumstances when massive software breaches are known and documented, recounts are necessary and appropriate to remove all potential doubt and to set an example for security best practices in all elections.

In 2022, records, video camera footage, and deposition testimony produced in a civil case in Georgia[1] disclosed that its voting system, used statewide, had been breached over multiple days by operatives hired by attorneys for Donald Trump.[2],[3] The evidence showed that the operatives made copies of the software

[1] No. 17-cv-02989-AT (N.D. Ga. filed Aug. 8, 2017).
[2] 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/
[3] Kate Brumback, "Video fills in details on alleged Ga. election system breach," *The Associated Press,* (September 6, 2022). Available at: https://apnews.com/article/2022-midterm-elections-technology-donald-trump-voting-92c0ace71d7bee6151dd33938688371e

that runs all of the equipment in Georgia, and certain other states, and shared it with other Trump allies and operatives.[4]

Subsequent court filings and public records requests revealed that the breaches in Georgia were part of a larger effort to take copies of voting system software from systems in Michigan,[5] Pennsylvania,[6] Colorado[7] and Arizona,[8] and to share the software in the operatives' network. According to testimony[9] and declarations[10] by some of the technicians who have obtained copies of the software, they have had access for more than three years to the software for the central servers, tabulators, and highly restricted election databases of both Election Systems & Software (ES&S), and Dominion Voting Systems, the two largest voting system vendors, constituting the most severe election security breach publicly known.

Combined, their equipment counts nearly 70% of all votes nationwide. Ninety-six percent of Arizona voters use Dominion and ES&S equipment; 100% of Georgia voters vote on Dominion machines; 98% of Nevada votes on Dominion voting machines and the remainder uses ES&S; 69% of Michigan voters' ballots are counted on Dominion or ES&S equipment; 89% of Pennsylvania voters ballots

---

[4] Emma Brown, Jon Swaine, "Inside the secretive efforts by Trump allies to access voting machines," *The Washington Post*, (October 28, 2022). Available at: https://www.washingtonpost.com/investigations/2022/10/28/coffee-county-georgia-voting-trump/

[5] Clara Hendrickson, "Did data from Georgia voting machine breach play a role in alleged Michigan election plot?", *The Detroit Free Press,* (August 31, 2023). Available at: https://www.freep.com/story/news/politics/2023/08/31/michigan-and-georgia-voting-machine-breach-connection/70702597007/

[6] Jeremy Duda, "Group led by 'kraken' lawyer Sidney Powell hired the firm recounting AZ's election to probe election in Fulton Co." *Pennsylvania Capital-Star*, (May 24, 2021). Available at: https://penncapital-star.com/government-politics/group-led-by-kraken-lawyer-sidney-powell-hired-the-firm-recounting-azs-election-to-probe-a-pa-election/

[7] Christina A. Cassidy, "Georgia election indictments highlights wider attempts to illegally access voting equipment," *Associated Press*, (August 15, 2023). Available at: https://apnews.com/article/georgia-trump-indictment-voting-machines-conspiracy-theories-bc3db57cabd25fd8e335f85ed299e79c

[8] Maritsa Georgiou, "Arizona voting system data sent to Montana lab as part of the latest audit," *NBC Montana,* (June 3, 2021). Available at: https://nbcmontana.com/news/local/arizona-voting-system-data-sent-to-montana-lab-as-part-of-latest-audit

[9] *See eg.,* Lenberg Dep. No. 17-cv-02989-AT Document 1613, page 101-102. Available at: https://www.dropbox.com/s/t9pkebeb44dg3it/Ex%2024%20%201613%20Depo%20Jeffrey%20Lenberg.pdf?dl=0

[10] Michigan 6th Circuit Court Oakland Case No. 2023-285759-FH, MTN to Quash, Sep. 30, 2024. Pages 188, 240-241, 295 and 298. Available at: https://freespeechforpeople.org/wp-content/uploads/2024/11/20240930_motion_fld_to_quash_indictment-dft_104715112_ocr.pdf

are counted on Dominion or ES&S equipment; ES&S counts 92% of North Carolina ballots; and either ES&S or Dominion counts 97% of Wisconsin votes.[11]

Possessing copies of the voting system software enables bad actors to install it on electronic devices and to create their own working replicas of the voting systems, probe them, and develop exploits. Skilled adversaries can decompile the software to get a version of the source code, study it for vulnerabilities, and could even develop malware designed to be installed with minimal physical access to the voting equipment by unskilled accomplices to manipulate the vote counts. Attacks could also be launched by compromising the vendors responsible for programming systems before elections, enabling large scale distribution of malware.

In December 2022[12] and again in 2023,[13] many of us, concerned by the security risks posed by these breaches, wrote to the Attorney General, FBI Director, and Cybersecurity and Infrastructure Security Agency (CISA) Director outlining the security concerns and urging an investigation. Though there have been limited, localized investigations,[14] there is no evidence of a federal investigation[15] to determine what was done with the misappropriated voting software.

Other relevant parties have pointed to the serious risks posed by the misappropriation of the voting software. Before it was known that partisan operatives had taken the software, Dominion Voting Systems objected vehemently to providing its software to the same partisan actors who ultimately got copies through voting system breaches, stating that to give its software to biased actors would cause "irreparable damage" to the "election security interests of the country."[16]

---

[11] See: https://verifiedvoting.org/verifier/#mode/navigate/map/makeEquip/mapType/normal/year/2024

[12] Available at: https://freespeechforpeople.org/wp-content/uploads/2022/12/doj.fbi_.dhs_.coffee.ga_.12.12.2022.pdf

[13] Available at: https://freespeechforpeople.org/wp-content/uploads/2023/12/doj.fbi_.coffee12.4.23.pdf

[14] Joey Cappelletti, "Trump allies who 'orchestrated' plan to tamper with voting machines face charges in Michigan," *Associated Press*, (August 3, 2023). Available at: https://apnews.com/article/stefanie-lambert-trump-michigan-election-fraud-bf9608af4b0972d41b5f4d303f5f6a29

[15] Sarah Wire, "Are the feds ignoring Trump allies' multistate effort to access voting systems? Experts raise alarms for 2024," *Los Angeles Times*, (March 9, 2023). Available at: https://www.yahoo.com/entertainment/anyone-investigating-trump-allies-multi-100017273.html

[16] Jonathan J. Coorper, "Arizona senate issues new subpoena for 2020 election audit," *Associated Press*, (July 27, 2021). Available at: https://apnews.com/article/joe-biden-government-and-politics-arizona-senate-elections-election-2020-e7e26601f50611195fd47a3ffb92c311

Before the breaches in Georgia had been confirmed, the Georgia Secretary of State's chief information officer testified that having copies of the software would provide a "road map" to the ways the system could be accessed.[17] The Georgia Attorney General opposed providing copies of the software to lawyers for the Trump campaign in a late 2020 election challenge, arguing that images of the voting system software would provide "the keys to the software kingdom."[18]

Notably, U.S. elections are potentially resilient because there are paper ballots recording the voters' intent in most states, meaning that even if the voting system is at risk, the will of the voters can be determined reliably by recounting the paper ballots by hand (although we are aware that not all paper ballots are verified by the voter, and not all states take adequate care to protect the ballot chain of custody.)

Audits will be conducted in some of the most scrutinized states, but in key states they will not be conducted in a timely way that could reveal any concerns with the vote count. In addition, in most states the audits are insufficiently rigorous to ensure any potential errors in tabulation will be caught and corrected, and they cannot be considered a safeguard against the security breaches that have occurred. Specifically, Georgia's audits are non-binding, and Michigan, Nevada and Wisconsin laws do not provide that the audit be conducted before certification. Therefore, it would be impossible to know for these critical states if the audits uncovered errors or miscalculations before the state deadlines to seek recounts.[19]

Among swing states, only Arizona's audit laws ensure that, if enough discrepancies are identified, the audit hand count will be expanded to correct a potentially incorrect result. In other words, aside from Arizona, in contested states, there is no legal mechanism for the audit to correct the outcome, no matter how much error the audit uncovers. Given these facts, the only guarantee for rigorous, effective audits of the vote in the swing states will be through candidate-requested statewide hand recounts.

The facts around the voting system breaches are not disputed; it is well-documented that there were severe, multiple voting security breaches before the 2024 election. To ensure that voters can have confidence that the breaches in

---

[17] *See:*. No. 17-cv-02989-AT Beaver Dep Document 1368-3 Page 157-158.
[18] No.1:20-cv-04809-TCB (N.D. Ga filed Nov. 30, 2020), Document 23, page 13. Available at: https://www.dropbox.com/scl/fi/xlvuqfqroogx7vg1sa4p9/Pearson-transcipt-gov.uscourts.gand.284055.23.0-Clean.pdf?rlkey=aghdw5w34rwqxugdxhnk8ij5b&e=1&dl=0
[19] See: Verified Voting Audit Law Database at: https://verifiedvoting.org/auditlaws/

security did not taint the results of the 2024 election, we recommend pursuing hand recounts in, at minimum, Michigan, Nevada, Wisconsin and Pennsylvania as they will provide insufficient safeguards against threats posed by the breaches of the election software and will not provide important information in a timely way.

Thank you for your time and consideration of this important matter.

Sincerely,

Duncan Buell Ph.D.
Chair Emeritus — NCR Chair in Computer Science and Engineering
Dept. of Computer Science and Engineering
University of South Carolina*

David Jefferson Ph.D.
Lawrence Livermore National Laboratory* (retired)
Election Integrity Foundation*

Susan Greenhalgh
Senior Advisor for Election Security
Free Speech For People

Chris Klaus
Founder
Internet Security System*

William John Malik
Malik Consulting, LLC*

Peter G. Neumann Ph.D.
Chief Scientist,
SRI International Computer Science Lab*

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

*Affiliations are listed for identification purposes only and do not imply institutional endorsement.