EXHIBIT 5

Declaration of J. Alex Halderman (Sept. 21, 2021)

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF** **J. ALEX HALDERMAN** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. My July 1, 2021, expert report describes numerous security vulnerabilities in Georgia's Dominion ICX BMDs. These include flaws that would allow attackers to install malicious software on the ICX, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems. They are not general weaknesses or theoretical problems, but

rather specific flaws in the ICX software, and I am prepared to demonstrate proof-of-concept malware that can exploit them to steal votes cast on ICX devices.

3. Some of these critical vulnerabilities could be at least partially mitigated through changes to the ICX software if Dominion implemented such changes and jurisdictions deployed them. However, it would likely take months for Dominion to assess the problems, develop responsive software updates, test them, obtain any necessary approvals from the EAC and state-level certification authorities, and distribute the new software to states, as well as additional time for localities to install the changes. But Dominion cannot begin this process, because (to my knowledge) they have yet to learn what is in my report.

4. My analysis also concludes that the ICX is very likely to contain other, equally critical flaws that are yet to be discovered. Jurisdictions can mitigate this serious risk through procedural changes, such as reserving BMDs for voters who need or request them. Election officials cannot make an informed decision about such urgent policy changes or any other mitigations until they have assessed the technical findings in my report. However, to my knowledge, the Georgia Secretary of State's Office has yet to even request access to it, despite Plaintiffs' repeated offers to make it available to appropriate individuals at the Secretary's Office.

5. Nor do these problems affect Georgia alone. In 2022, the ICX will be used in parts of 16 states.[1] Nevada will use it as the primary method of in-person voting in certain areas of the state. Louisiana is slated to use it for early voting in a DRE configuration where there is not even a paper trail. It will be used for accessible voting in Alaska and large parts of Arizona, California, Colorado, and Michigan. It will also see some use in parts of Illinois, Kansas, Ohio, Missouri, New Jersey, Pennsylvania, Tennessee, and Washington State. Officials in these jurisdictions too must act to update the software and their procedures, but they cannot do so without information about the problems. Continuing to conceal those problems from those who can—and are authorized to—address them, to the extent possible, serves no one and only hurts voters (and heightens the risk of compromise in future elections).

6. The most effective way to ensure that the necessary information gets to the parties responsible (without also falling into the wrong hands) would be to share my report with the Cybersecurity and Infrastructure Security Agency (CISA), which operates a Coordinated Vulnerability Disclosure (CVD) program for just this purpose. CISA is a federal agency that collaborates with state and local governments, election officials, federal partners, and vendors to manage risks to U.S. election

[1] See Verified Voting, "Verifier Search – November 2022," https://verifiedvoting.org/verifier/#mode/search/year/2022/model/ImageCast%20X.

infrastructure.[2] Under CISA's CVD process, agency staff would independently validate the vulnerabilities, work with Dominion to develop software updates as necessary, and facilitate sufficient time for affected states and localities to apply mitigation strategies.[3] CISA strives to disclose "accurate, neutral, objective information focused on technical remediation and mitigation" and to "correct misinformation where necessary,"[4] making it well qualified to coordinate the disclosure of such sensitive vulnerabilities.

7. Geoff Hale, Director of CISA's Election Security Initiative, has confirmed to me that, if the Court permits it, the agency would be willing to receive my expert report and carry out coordinated vulnerability disclosure activities as appropriate (see Exhibit 1). Mr. Hale requests that I and my assistant Drew Springall be available for consultation with CISA during the CVD process, which we would be willing to do subject to the Court's permission.

8. Informing responsible parties about the ICX's vulnerabilities is becoming more urgent by the day. Foreign or domestic adversaries who are intent on

---

[2] Cybersecurity and Infrastructure Security Agency, "Election Infrastructure Initiative," https://www.cisa.gov/election-security.
[3] Cybersecurity and Infrastructure Security Agency, "Coordinated Vulnerability Disclosure Process," https://www.cisa.gov/coordinated-vulnerability-disclosure-process.
[4] *Id.*

attacking elections certainly could have already discovered the same problems I did, yet Georgia's 2022 primaries are less than nine months away, and other states that use the ICX will conduct high-profile elections even sooner. It is important to recognize the possibility that nefarious actors already have discovered the same problems I detail in my report and are preparing to exploit them in future elections. Providing my report to CISA through its CVD program will ensure that Dominion and affected jurisdictions are able to begin appropriate mitigations as soon as possible. Continuing to withhold my report from CISA puts voters and election outcomes in numerous states at unnecessary, and avoidable, risk.

9. I understand that State Defendants object to disclosure to CISA on the argument that my report should be used only for this lawsuit. But this ignores the implications of my report and my role in this matter. I am not a party to this lawsuit. I am an independent expert who was engaged to conduct an impartial assessment of the security and reliability of the Dominion BMD system, using (in part) election equipment that the Court ordered I be provided. I have done that, as reflected in my lengthy, detailed report and other submissions in this matter. As an independent expert and member of the election integrity community, I have a professional obligation to take appropriate steps to ensure that the severe vulnerabilities my report describes are properly remediated, to the extent possible, and that those tasked with

election security and administration across the country have the information they need to make responsible, informed decisions about election procedures, including the equipment used, the manner and purposes for which it is used (including whether it is used at all), the steps needed to secure that equipment and other aspects of the election systems in which it is used, and more. In short, my professional obligations do not end at the boundaries of this lawsuit, nor do the serious risks to voters and elections that my report discusses in depth. Additionally, I can imagine no prejudice to anyone in this lawsuit (or beyond) from disclosure of my report to CISA, nor am I aware of any claim of prejudice from any of the parties.

10. I of course have complied, and will continue to comply, with all directives from the Court regarding disclosure of my work in this matter. I submit this declaration to explain why I believe disclosure of my report to CISA is critically important (and not just for Georgia) and to respectfully ask that the Court allow that disclosure, rather than accept State Defendants' position that my findings must not be shared beyond the confines of this lawsuit, including with those who are authorized to address the vulnerabilities with the ICX and stand ready to do so. If my findings regarding the ICX actually present no meaningful risks to voters and election outcomes and therefore require no remediation, as I gather State Defendants would have the Court believe, CISA is well positioned to determine that. If, on the other

hand, my findings do warrant remediation, as I believe they do, then CISA is well positioned to work with Dominion and the appropriate authorities around the country to implement remedial measures. I can see no reason to prevent (or further delay) that important work for future elections. And I note that none of State Defendants' experts have disputed my findings regarding the ICX machines. Only Dr. Juan Gilbert has responded to my sealed report, and he has not examined the machines (or used them) to my knowledge.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 21st day of September, 2021 in Ann Arbor, Michigan.

J. ALEX HALDERMAN

Gmail J. Alex Halderman <halderman@gmail.com>

Vulnerability Disclosure

Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov> Thu, Aug 19, 2021 at 12:15 PM
To: "J. Alex Halderman" <jhalderm@umich.edu>
Cc: Andrew Springall <andrew.springall@gmail.com>

Prof. Halderman,

Thank you for your email. Yes, CISA would be willing to receive the report regarding possible vulnerabilities in election infrastructure for inclusion in CISA's Coordinated Vulnerability Disclosure (CVD) process and would carry out any further coordinated disclosures activities as appropriate. As we share on our public website (https://www.cisa.gov/coordinated-vulnerability-disclosure-process), CISA's CVD program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). Note that part of our process may also involve validating any alleged vulnerabilities, planned mitigations, remediations, or patches with the security researcher who discovered the alleged vulnerability, so we would appreciate if you could continue to be available for consultation during the CVD process as well.

As shared on our website, please submit any vulnerability reports for CVD coordination using the form here: https://www.kb.cert.org/vuls/report/

Best,

Geoff

From: J. Alex Halderman <jhalderm@umich.edu>
Sent: Wednesday, August 18, 2021 4:37 PM
To: Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>
Cc: Andrew Springall <andrew.springall@gmail.com>
Subject: Vulnerability Disclosure

Dear Mr. Hale,

We are writing to you in your capacity as Director of the Election Security Initiative at the federal Cybersecurity and Infrastructure Security Agency (CISA).

We understand that the Election Security Initiative at CISA works to ensure the physical security and cybersecurity of the systems and assets that support the Nation's elections, including through detection and prevention, information sharing and awareness, and incident response.

As you may be aware from recent press reports, one of us (Halderman) is presently serving as an expert witness for the plaintiffs in Curling v. Raffensperger (Civil action no. 1:17-CV-2989-AT, N.D. Ga.), a case that concerns the security of Georgia's election system. A year ago, the court granted plaintiffs access to an ICP ballot scanner and ICX ballot marking device as used in Georgia in order to test their security. Following months of analysis, on July 1, Dr. Halderman submitted an expert report that describes several very serious vulnerabilities we found in the equipment, which, to our knowledge, have not been previously documented or disclosed.

Given the nature of the vulnerabilities and the time that would be necessary to mitigate them before the 2022 midterm elections, we believe it is critical for Dominion and affected jurisdictions (which include Georgia and parts of many other states) to begin taking responsive action soon. It is also vitally important to prevent information sufficient to exploit the vulnerabilities from falling into the wrong hands, and to avoid fueling election-related misinformation if possible.

Currently, disclosure of the expert report to anyone other than outside litigation counsel for the parties is strictly prohibited by the Court’s protective order and by recent directives from the judge. However, if permitted by the Court, we would like to share the report with CISA and ask your agency to carry out appropriate further disclosure of the information it contains to Dominion and affected jurisdictions as you see fit, under CISA's coordinated vulnerability disclosure (CVD) program (https://www.cisa.gov/coordinated-vulnerability-disclosure-process).

We understand that under this process, CISA will work with the vendor (Dominion) for mitigation development and the issuance of patches or updates and to facilitate sufficient time for affected end users to obtain, test, and apply mitigation strategies. We further understand that CISA strives to disclose "accurate, neutral, objective information focused on technical remediation and mitigation" and to "correct misinformation where necessary".

Please confirm that CISA would be an appropriate agency to handle coordinated vulnerability disclosure for election infrastructure under these circumstances, and that you would be willing to receive the report (subject to the Court's permission) and carry out further disclosures as you deem appropriate.

Sincerely,

J. Alex Halderman

Drew Springall