- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Vulnerabilities

Feds Oppose Immediate Release of Voting Machine Report

By Associated Press on February 11, 2022

A federal cybersecurity agency is reviewing a report that alleges security vulnerabilities in voting machines used by Georgia and other states and says the document shouldn't be made public until the agency has had time to assess and mitigate potential risks.

The report has been under seal since July in federal court in Atlanta, part of a long-running lawsuit challenging Georgia's voting machines. Its author, J. Alex Halderman, said in sworn declarations filed publicly with the court that he examined the Dominion Voting Systems machines for 12 weeks and identified "multiple severe security flaws" that would allow bad actors to install malicious software.

Plaintiffs in the case, who are election security advocates and individual voters, have for months called for the release of a redacted version of the report and urged that it be shared with state and federal election security officials. Lawyers for the state had repeatedly objected to those requests, but Secretary of State Brad Raffensperger last month put out a news release calling for its release.

[Read: Experts Warn of Dangers From Breach of Voter System Software **]**

U.S. District Judge Amy Totenberg agreed on Feb. 2 that the report could be shared with the U.S. Cybersecurity and Infrastructure Agency, or CISA. The agency said in a court filing Thursday that it would work with Halderman and Dominion to analyze potential vulnerabilities, develop any

necessary mitigation measures and work with jurisdictions that use the machines to test and apply any protections.

CISA said it would complete its "coordinated vulnerability disclosure" process as quickly as possible, but urged the judge not to release the report before it's done, saying "premature disclosure of Dr. Halderman's report, even in redacted form, could, in the event any vulnerabilities ultimately are identified, assist malicious actors and thereby undermine election security."

The report was initially designated "attorneys' eyes only," meaning even the actual parties to the lawsuit couldn't see it — only their lawyers and expert witnesses could. Halderman, a voting technology specialist and director of the University of Michigan's Center for Computer Security and Society, urged the court to make his findings public in a limited and responsible way so that problems could be addressed.

Halderman told The Associated Press in August that he'd seen no evidence that the machines' vulnerabilities were used to tamper with the 2020 election, but he said "there remain serious risks that policymakers and the public need to be aware of."

Totenberg has resisted making the report public, saying she too is concerned it could be exploited by attackers.

Raffensperger's news release went out Jan. 27 while the lawyers in the case were on a conference call with Totenberg. Noting that all parties in the case had come to agree that the report should be made public, an attorney for the plaintiffs asked the judge to release a version redacted by Halderman to exclude details showing how hacks could be carried out.

In a Feb. 2 phone call, Totenberg agreed that the report could be released to CISA but did not immediately decide whether it could otherwise be made public. She instructed the parties to talk with the federal agency to get information about its review, saying she wanted to know whether CISA would provide any guidance as to what should and shouldn't be disclosed.

Lawyers for the plaintiffs suggested that Totenberg make a redacted version of the report public 30 days after CISA received the unredacted version. A lawyer for the state didn't object to CISA getting the report, but said the public release should not be delayed, arguing that keeping it sealed undermines confidence in the election system.

Raffensperger said during an Atlanta Press Club event Thursday that Halderman had unlimited access to the touchscreen ballot-marking machines and was given the security codes, so he wasn't operating in "the real world." Halderman wrote in a declaration for the court that attackers could install malicious software "either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems."

The lawsuit alleges that Georgia's voting machines are not secure and should be replaced with hand-marked paper ballots. Halderman, an expert witness for the plaintiffs, is a staunch supporter of hand-marked paper ballots.

Others have also sought access to the report. Totenberg last month rejected a request for access from the secretary of state in Louisiana, which uses the Dominion system for early voting. She has not yet ruled on requests for access from Fox News and One America News, both of which are facing defamation suits filed by Dominion.

CISA said in its court filing that it "understands and shares the parties' urgency with completing this work, and will prioritize its completion as expeditiously as possible." It proposed that it would notify the court within 30 days about its progress, its timeline and its thoughts on the "scope and information to be included in a future public disclosure."

Read: [Report Highlights Cyber Risks to US Election Systems]