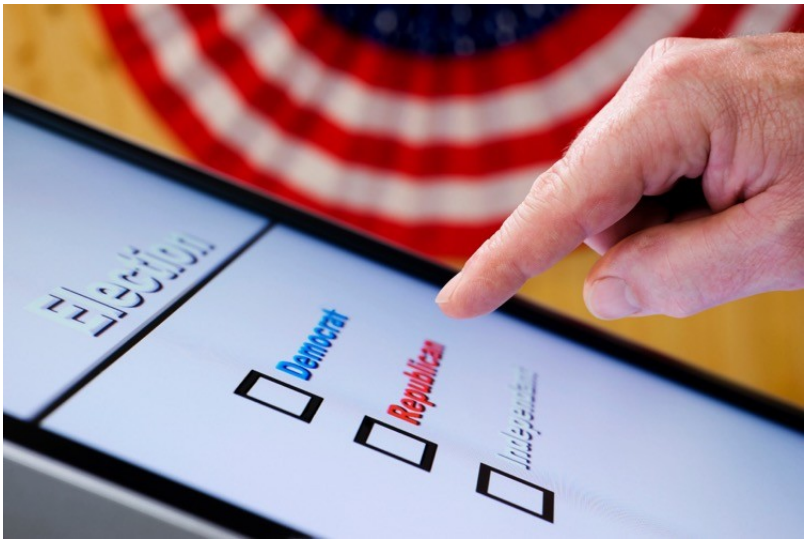
Written by **William F. Jasper** on June 3, 2022

# Federal Cyber Officials Admit: Dominion Voting Machines Vulnerable to Hacking, Fraud



cmannphoto/iStock/Getty Images Plus

"Electronic voting machines from a leading vendor used in at least 16 states have software vulnerabilities that leave them susceptible to hacking if unaddressed, the nation's leading cybersecurity agency says in an advisory sent to state election officials." So reported Associated Press on May 31 regarding an "advisory" issued by the federal Cybersecurity and Infrastructure Agency (CISA) to state officials. The Associated Press obtained a copy of the document, which has not yet been released to the public.

The CISA advisory, reports AP, focused on Dominion Voting Systems and "details nine vulnerabilities and suggests protective measures to prevent or detect their exploitation."

According to the AP article, the advisory is based on a report by Professor J. Alex Halderman, a renowned computer scientist at the University of Michigan, who, along with his students, is famous for "white hat" computer hacking that has exposed major security vulnerabilities in personal, commercial, and government computer systems. The AP report notes that "Halderman has long argued that using digital technology to record votes is dangerous because computers are inherently vulnerable to hacking and thus require multiple safeguards that aren't uniformly followed. He and many other election security experts have insisted that using hand-marked paper ballots is the most secure method of voting and the only option that allows for meaningful post-election audits."

"These vulnerabilities, for the most part, are not ones that could be easily exploited by someone who walks in off the street, but they are things that we should worry could be exploited by sophisticated attackers, such as hostile nation states, or by election insiders, and they would carry very serious consequences," Halderman told the AP.

The vulnerabilities that worry Dr. Halderman are the same weaknesses that election expert Lieutenant Colonel Kurt Hyde (Ret.) and Dr. Douglas Frank have been warning about concerning the 2020 presidential election. Lt. Col. Hyde, an elections historian and former adjunct instructor teaching a systems analysis course, was one of the earliest critics of electronic voting, pointing out since the mid-1980s that the move toward electronic ballots and away from an auditable paper trail was a dangerous trend. Dr. Franks, a physicist, mathematician, computer scientist, inventor, and former professor, has spent the better part of the past two years analyzing voter data, testifying before legislatures, and speaking to audiences across the nation on the manner in which the voting machine vulnerabilities and voter databases were exploited during the 2020 election to dramatically and illegally shift the vote in favor of Joe Biden. (This writer conducted a combined video interview with Lt. Col.

Hyde and Dr. Frank last August in Sioux Falls, South Dakota, at the Cyber Symposium sponsored by My Pillow founder Mike Lindell. See the Col. Hyde/Dr. Frank interview below)

In response to an inquiry from *The New American* about the significance of Dr. Halderman's recent analysis of Dominion voting machine vulnerabilities, Lt. Col. Hyde said this is "very welcome and timely news." "Professor Halderman is one of the top names in computer security issues," he told *The New American*, "and this reinforces the concerns that many leading authorities have expressed for years. Halderman, I don't believe, is a conservative or a Trump supporter. In fact, I think he tends to be liberal and probably a Democrat, but he's generally recognized to be a top-notch scientist who honestly follows the evidence. This is another important confirmation of the problems inherent in digital voting that many experts have been warning about for decades."

More from the Associated Press report:

> One of the most serious vulnerabilities could allow malicious code to be spread from the election management system to machines throughout a jurisdiction, Halderman said. The vulnerability could be exploited by someone with physical access or by someone who is able to remotely infect other systems that are connected to the internet if election workers then use USB sticks to bring data from an infected system into the election management system.
>
> Several other particularly worrisome vulnerabilities could allow an attacker to forge cards used in the machines by technicians, giving the attacker access to a machine that would allow the software to be changed, Halderman said.
>
> "Attackers could then mark ballots inconsistently with voters' intent, alter recorded votes or even identify voters' secret ballots," Halderman said.

Dominion Voting Systems claims that it has fixed the problems addressed by Halderman, but Halderman says that as far as he knows, "no one but Dominion has had the opportunity to test their asserted fixes."

While acknowledging  the vulnerabilities pointed out by Dr. Halderman, federal CISA officials are sticking to the narrative of the past two years that there is no evidence that these weaknesses were exploited to change the vote. CISA is also attempting to assure voters that there is no great danger from these vulnerabilities. According to the AP report, CISA Executive Director Brandon Wales said in a statement that "states' standard election security procedures would detect exploitation of these vulnerabilities and in many cases would prevent attempts entirely."

However, it should be remembered that this is the same politicized CISA run by Deep State operative Chris Krebs who, despite voluminous evidence to the contrary, proclaimed that the 2020 presidential election was "the most secure in American history," and that there was "no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised."

Related articles and videos:

"2000 Mules" Full of Must-See Surprises

Media Darling and Fired Cyber Security Chief Chris Krebs Is a Deep State Operative

Uncovering the Coverup

LINDELL CYBER SYMPOSIUM: Dr. Douglas Frank and Col. Kurt Hyde on Election Fraud and Election

Integrity 8-20-21

Congressman Nunes: “Electronic Voting Systems … Are Really Dangerous”

Voter Fraud – Interview with the Author

Dangers of Internet Voting

Voting on the Web

Will the 2010 U.S. Census Data Be Used to Fraudulently Register Voters?