

BREAKING: Tulsi Gabbard Drops Bomb on Voting Machines — Says Evidence Shows Voting Machines Can Be Tampered With to Steal Elections

GP thegatewaypundit.com/2025/04/tulsi-gabbard-drops-bomb-voting-machines-says-evidence/

Apr. 10, 2025 1:13 pm



Screenshot

In a jaw-dropping moment during a high-level Cabinet meeting on Wednesday, United States Director of National Intelligence Tulsi Gabbard dropped a bombshell: there is now evidence that electronic voting machines have been tampered with to manipulate election outcomes in the United States.

Gabbard gave a detailed update on her sweeping investigations into the politicization of intelligence and election interference.

Her statement confirmed what many conservatives have long suspected — that the very foundations of America’s electoral system have been compromised.

“I’ve got a long list of things that we’re investigating. We have the best going after this, election integrity being one of them,” Gabbard said.

“We have evidence of how these electronic voting systems have been vulnerable to hackers for a very long time and vulnerable to exploitation to manipulate the results of the votes being cast, which further drives forward your mandate to bring about paper ballots across the country so that voters can have faith in the integrity of our elections.”

WATCH:

This should not come as a surprise to readers of The Gateway Pundit, who have been following our report.

Even the world’s leading hackers concur with this assessment.

Last year, some of the world’s top hackers convened in Las Vegas for the annual DEF CON conference, specifically at the Voting Village event, to probe and expose vulnerabilities in voting machines set to be used in the upcoming November election.

From Friday through Sunday, hackers at Voting Village tested various voting machines and related equipment, attempting to bypass security measures.

Harri Hursti, co-founder of Voting Village, noted that the list of vulnerabilities found was extensive but consistent with previous years.

“There’s so much basic stuff that should be happening and is not happening, so yes I’m worried about things not being fixed, but they haven’t been fixed for a long time, and I’m also angry about it,” Hursti told Politico.

Scott Algeier, executive director of the Information Technology-Information Sharing and Analysis Center (IT-ISAC), emphasized that fixing vulnerabilities is not a quick process: “Even if you find a vulnerability next week in a piece of modern equipment that’s deployed in the field, there’s a challenge in getting the patch and getting the fix out to the state and local elections officials and onto the equipment before the November election.”

“It’s not a 90-day fix, It’s not a Microsoft every Tuesday, issue your patch and everything works fine. It’s a pretty complicated process,” he added.

This is not the first time Def Con hackers were able to penetrate vulnerable voting machines used in the US today.

In July 2017, the DEF CON hackers made quick work of the voting machines. Hackers were given the rare chance to crack into US voting machines. It took one person just 90 minutes to hack in and vote remotely on one of the machines.



Watch Video At: <https://youtu.be/4p4mXCn470s>

Here's another detailed video from 2017:



Watch Video At: <https://youtu.be/clf8eTSBL3Y>

In **2019**, at the **DEF CON** conference in Las Vegas, NBC News' technology correspondent Jacob Ward provided an in-depth look at how easily hackers can exploit vulnerabilities in voting systems.



Watch Video At: <https://youtu.be/QtWP0KDx2hA>

This is not the first time we have heard about election machine vulnerabilities.

In 2023, University of Michigan Professor of Computer Science and Engineering J. Halderman, revealed in a Georgia courtroom that Dominion Voting Systems were vulnerable to hacks.

Trending: BOOM! President Trump Shuts Down “Very Low-Rated” Kaitlin Collins During Press Conference with El Salvadorian President – Stephen Miller, Bondi, Rubio, and Nayib Bukele SCHOOL Her in Epic Exchange (VIDEO)

His report confirmed that votes can be altered in the Dominion voting machines. In fact, the report reveals that the Dominion software is vulnerable and can be hacked.

Professor Halderman wrote in his report:

We discovered vulnerabilities in nearly every part of the system that is exposed to potential attackers. The most critical problem we found is an arbitrary-code-execution vulnerability that can be exploited to spread malware from a county’s central election management system (EMS) to every BMD in the jurisdiction. This makes it possible to attack the BMDs at scale, over a wide area, without needing physical access to any of them.

Our report explains how attackers could exploit the flaws we found to change votes or potentially even affect election outcomes in Georgia.

The Secretary of State in Georgia, Brad Raffensperger, announced in 2023 that he would not fix the vulnerabilities before the 2024 election.

Astonishingly, Georgia Secretary of State Brad Raffensperger, who has been aware of our findings for two years, just announced that the state will not get around to installing Dominion's security patches until after the 2024 Presidential election.

<https://t.co/bnPXoP6Xc2>

— J. Alex Halderman (@jhalderm) June 14, 2023

Dr. Halderman revealed that the Dominion machines were so vulnerable that he was able to hack into one of the machines in the courtroom with a pen!

The Gateway Pundit has published dozens of reports like this over the past decade. Unfortunately, nothing ever changes. Republicans turn their back and walk away. And Americans continue to use vulnerable voting machines in election after election.