Maryland Voter Integrity Group Recommends the State Move to Paper Ballots with a Hand Count After Voting Machine Vulnerabilities Exposed by Arizona Audit

The organization seeks support from concerned Marylanders to stamp out fraud and return to free, fair, and transparent elections

ROCKVILLE, MD – October 12, 2021 –Maryland Voter Integrity Group announces today that its community has gathered insights and information to call into question that voting machines are not connected to the Internet and therefore cannot be hacked.

In the case of the recent Arizona audit, Sonny Borelli, Retired Marine Gunnery Sergeant and Arizona State Senator for Legislative District 5 and Matt Salmon, Former Congressman and Gubernatorial Candidate in Georgia, raise a number of concerns. Citing cases of deleted files, destroyed evidence, and systems connected to the Internet when officials repeatedly said they would not be, have added to the distrust among voters that the election, and subsequent audit itself in Arizona, were legitimate. Matt Salmon continued to say in a recent interview that in addition to systems being Internet-enabled, no multi-factor authentication or unique passwords were used, which he feels enabled potentially criminal activity.

The recent Maricopa County, AZ Audit Report notes a number of troubling findings, including:

- **57K questionable votes**, deleted election files, and suspicious voting machine activity;
- **10,000+ double votes across county lines**, as well as votes from deceased voters, voters who are not listed in public records, and those who are identifiable as the same person with two different Voter IDs;
- **Tens of thousands of ballots cast from individuals who had moved prior to the election and could not have physically received their ballots, legally**;
- **Proper voter registration law and procedures were not followed**, leading to unexplained large purges of registered voters, right after the election, of people who had voted in the election and back dating of registrations, adjustments made to historical voting and voter records, unexplained linking of voter registration affidavits to multiple voters and more;
- **Files were missing** from the Election Management System (EMS) Server;
- **Ballot images on the EMS were corrupt or missing**;
- **Logs appeared to be intentionally rolled over**, and all the data in the database related to the 2020 General Election had been fully cleared;
- **Ballot batches were not always clearly delineated**, duplicated ballots were missing the required serial numbers, originals were duplicated more than once, and the Auditors were never provided Chain-of- Custody documentation for the ballots for the time-period prior to the ballot's movement into the Auditors' care. This all increased the complexity and difficulty in properly auditing the results; and
- **Several anomalies noted in the ratio of hand-folded ballots, on-demand printed ballots, and an increase in provisional ballot rejections for a mail-in ballot already being cast**, which suggests that potentially mail-in ballots were cast on voters' behalves without their knowledge.

Kim Zetter, a recognized Cybersecurity and National Security journalist, recently added her expertise to clarify if – and specifically how – voting machines are vulnerable to hacking. As Borelli and Salmon mentioned, the conversation has long centered on election machines not being connected to the Internet, a fact that now has been broadly proven to be untrue. If anything, Kim notes, the rising pressure for fast results on election night has led to the use of Internet-enabled systems to capture and transfer voting data via the addition of cellular modems in the machines themselves.

According to Zetter, Election Systems and Software, the creator of the voting machines widely used across the U.S., has said that even if systems are Internet-enabled, they are secure because the modems are one-way, and no one is able to 'dial in.' However there has been no testing conducted at the federal level to confirm that this is the case – "ES&S doesn't have a good track record for implementing security." In January, 2020, NBC reported that ES&S installed 10,000 modems connecting their voting machines to the Internet.

An NBC report follows graduate engineering students at the University of Michigan. Led by Computer Science Assistant Professor Alex Halderman, they demonstrate just how easy it is to gain access to Internet-enabled election systems. In this same video, Halderman mentioned that "…Internet voting magnifies problems 100-fold…" and in less than 36 hours, his team of graduate students proved just how true that is. Using a 'shell injection attack,' a well-known hacker approach, one vulnerability in the DC election system from 2010 allowed them to gain full control of the server and have the ability to change votes.

"It is apparent that the significant anomalies that have been uncovered to-date and found to be statistically significant point to large-scale integrity and security issues at all levels of our election systems," Chair of the Maryland Voter Integrity Group, Robyn Sachs said. "With all that has been found to-date, we strongly recommend that the state of Maryland return to paper ballots with a hand-count to ensure our election integrity is upheld and as the best defense against fraud."

About The Maryland Voter Integrity Group

The Maryland Voter Integrity Group is committed to stamping out fraud and inaccuracies in Maryland's voter rolls to preserve voter confidence and free, fair, and transparent elections. For more information, please visit www.mdvoter.org and the organization's Facebook page.

By MDvoter.org | October 12, 2021 | Press Releases | 0 Comments