Colorado Clerk Tina Peters Releases Report – Claims Dominion Voting Machines Used in 2020 Election Were Illegally Certified and Illegally Configured

Description

USA: **Tina Peters, who was mercilessly attacked by the Soros-backed Colorado Secretary of State and the state media, recently released a report on the hard drives of the Dominion voting machines used in Colorado in the 2020 Election. This report has many shocking findings.**

Tina Peters is the election worker in Colorado who backed up the voting machines in her county when the corrupt Soros-backed Secretary of State demanded that all voting machines be altered in a manner that erased election data (which is against the law). Ms. Peters was attacked for her actions.

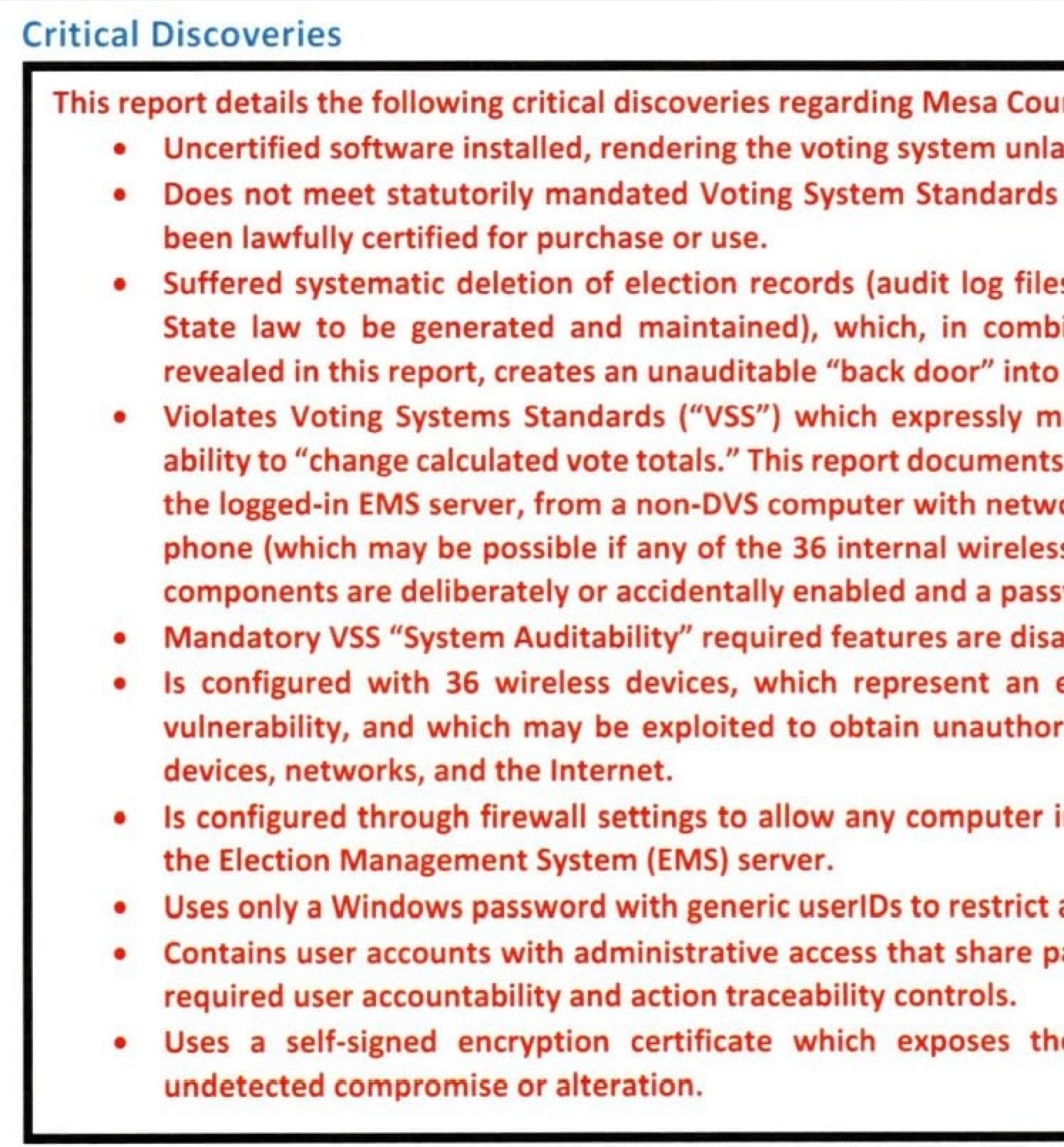
> FBI Raids Home of County Clerk and Whistleblower Tina Peters — The State Official Who Refused to Wipe Election Data from Computers Without Making a Copy

Advertisement – story continues below

Recently in early February Peters was interrupted at a local restaurant by police and arrested on some garbage charges. What are the chances that Peters is being harassed and attacked because she knew too much?

> Colorado Election Clerk Tina Peters Who Refused to Break the Law and Delete 2020 Data from Her County's Voting Machines Arrested on BS Charges

Ms. Peters recently sent a report to the state of Colorado with the results from an investigation into the Dominion voting machines used in her state in the 2020 Election. The report is damning. It shows that the county's voting machines were illegally certified and illegally configured in the 2020 Election. The report lists a number of significant issues in the executive summary of the report.



Critical Discoveries

This report details the following critical discoveries regarding Mesa Cou

- Uncertified software installed, rendering the voting system unla
- Does not meet statutorily mandated Voting System Standards
  been lawfully certified for purchase or use.
- Suffered systematic deletion of election records (audit log file
  State law to be generated and maintained), which, in comb
  revealed in this report, creates an unauditable "back door" into
- Violates Voting Systems Standards ("VSS") which expressly m
  ability to "change calculated vote totals." This report document
  the logged-in EMS server, from a non-DVS computer with netw
  phone (which may be possible if any of the 36 internal wireles
  components are deliberately or accidentally enabled and a pass
- Mandatory VSS "System Auditability" required features are disa
- Is configured with 36 wireless devices, which represent an
  vulnerability, and which may be exploited to obtain unautho
  devices, networks, and the Internet.
- Is configured through firewall settings to allow any computer
  the Election Management System (EMS) server.
- Uses only a Windows password with generic userIDs to restrict
- Contains user accounts with administrative access that share p
  required user accountability and action traceability controls.
- Uses a self-signed encryption certificate which exposes th
  undetected compromise or alteration.

By Joe Hoft

Category

1. Main
2. Politics-Geopolitics-Gov.-Events

Date Created
03/08/2022