BULLETIN
July 29, 2019
(404) 664-4044

Contact: Garland Favorito
garlandf@msn.com
http://www.voterga.org

New Vulnerabilities, Election Breach Cover-Up Revealed

ATLANTA GA – Georgia's voting system was on public trial again late last week. Bombshell testimony revealed new vulnerabilities and a cover-up after the 2017 server internet exposure in the Center for Election Systems (CES) at Kennesaw State University (KSU). **That vulnerable server was used to build ballots shown by all voting machines in all counties during all elections for about 13 years**.

Former CES director, now Assistant Elections Director, Michael Barnes, admitted that once he became aware of the server exposure, **he took no steps** to determine the cause, duration, what files were exposed, the extent of vulnerabilities or how to remediate them. **Barnes allowed KSU Information Technology staff to wipe the server clean in 2017** and did not inform them to preserve data that was subject to a litigation hold. His testimony confirmed findings in the 2017 VoterGA audit.

Merritt Beaver, Chief Information Officer (CIO) for the Secretary of State (SOS), further admitted that **no action was taken to cleanse any of 159 county servers that may still be compromised by malware from the internet exposure**.

In 2017, Beaver hired Fortalice to assess SOS security but **did not engage them to look at the vulnerable election system.** Instead, he directed them to look at the SOS data center server that handles corporations and licensing and a voter registration system. IN 2017, Fortalice found 22 significant risks in the SOS data center server. In 2018, they found 15 significant risks in the PCC voter registration system. Only three SOS server risks were remediated by the 2018 election. Theresa Payton of Fortalice testified **they did not assess CES, election servers, voting machines, memory cards or scanners although they have capabilities to do so.**

In 2018, SOS Brian Kemp brought CES in house but Barnes admitted **they hired three ES&S employees to build ballot files in their homes and transfer them though the internet to an SOS public server**. Barnes stated he puts a memory stick into a public server to get ballot files and then puts the stick into the elections server to upload them. The transfer can potentially infect the elections server.

SOS officials falsely contended for years that elections servers are "air gapped" and not connected to the internet. State's expert witness Michael Shamos admitted the new process is **not** air gapped. He further admitted the state should **not** obtain new ballot marking devices that embed votes in bar codes.