April 30, 2018

Contact: Garland Favorito
(404) 664-4044

Audit Reveals SOS "Cover-Up" in Elections Data Destruction

ATLANTA GA – VoterGA has released a new independent audit report with never before published information about the highly controversial destruction of Georgia election data last year at Kennesaw State University (KSU). The audit provides a detailed analysis that **disproves** a brief October 30th report from the Secretary of State (SOS) office claiming the data destruction was ***"standard procedure".*** That SOS report was produced just four days after Secretary Brian Kemp posted on his Facebook account and Twitter feed that KSU actions were ***"reckless behavior", "inexcusable conduct", "gross incompetence"*** **and** ***"undeniable ineptitude"***.

The audit cites over a dozen instances where the SOS report **ignored standard SOS election investigation procedures or failed to investigate critical aspects of the data destruction**. It also provides information from Open Records Requests showing **all three SOS report conclusions to be essentially false**. The audit cites the Center for Election Systems (CES) at KSU as culpable for exposing elections data, failing to secure the data, failing to back up the data, failing to follow SOS data retention policies and allowing elections data to be destroyed without a forensic risk assessment to identify sources and time frames of prior breaches.

The audit explains how Georgia's centralized election preparation allows a **single point of attack** on the key election server. The server contains voter information that counties **download,** elections databases that counties use to accumulate results and files that counties use to prep all their voting machines. The server exposure allowed any potential attacker to spread election mode malware to all counties and their voting machines **without physical access to a single voting machine**. That type of malware **cannot be detected** during logic and accuracy testing when the machines are in test mode. CES does not provide adequate procedures to counties so that they can validate the security of the data or files they receive from CES.

The audit concludes that the SOS report was **not credible** and that recent changes underway will not necessarily solve the problems faced. It goes on to explain that the exposure likely existed for years dating to when CES installed the elections server. Since CES personnel have always been under contract to the SOS office, which is responsible for overseeing their activities, the audit concludes that the SOS office is continuing in a **cover-up** to prevent the full truth from being known.

###