

Coalition for Good Governance

7035 Marching Duck Drive E504
Charlotte, NC 28210
704 552 1618

October 29, 2017

Re: Open Letter to Georgia Municipal, County, and State Election Officials

Dear Georgia Election Official:

November 7 elections conducted using Georgia's electronic voting system will be legally noncompliant and their results should not be certified. It is imperative that local officials immediately discontinue the use of the system in the current election. The disclosures of the last several days expose the fact that the voting system is compromised and cannot be relied on to produce accurate results.

Even Secretary of State Brian Kemp acknowledged Friday that the central server that touched all components and election programming was compromised¹ at the time the staff wiped the server's hard drive. Kemp, ducking responsibility for the massive security failures of the system under his control, blamed the "gross incompetence" of his election operations at Kennesaw State's ("KSU") Center for

¹ From <https://www.facebook.com/BrianKempGA/posts/10155101852781275>:

"The Secretary of State's office had no involvement in this decision, and we would never direct someone to take such action. This pattern of reckless behavior is exactly why we are ending our relationship with KSU and the Center for Elections Systems and moving functionality in-house.

"Not only did KSU officials fail to notify us of the server's vulnerabilities when they first learned of the problem, they failed again to notify us when they decided to wipe the compromised server and the back-up server. We will not stand for this kind of inexcusable conduct or gross incompetence.

"Earlier today, we opened an internal investigation on this new incident at KSU. Those responsible at KSU should be held accountable for their actions. The Secretary of State's office is also coordinating with FBI officials to get our own copy of the data that was erased at KSU.

"Despite the undeniable ineptitude at KSU's Center for Elections Systems, Georgia's elections are safe and our systems remain secure. As Secretary of State, I will continue to lead around the clock efforts to keep it that way."

Election Systems (“CES”) that many election integrity activists have warned of for years. CES is the Secretary of State’s contract agent responsible for programming the elections and maintaining secure and reliable election equipment. CES’s records and equipment are the records and property of the Secretary of State, not KSU. Secretary Kemp failed to take reasonable efforts to secure and preserve these records for which he had the duty to diligently maintain.

The new disclosures came in the wake of the shocking news that on July 7, one day after Secretary Kemp received a copy of our lawsuit (Curling v. Kemp), CES/KSU destroyed key evidence by wiping the hard drive of the main CES server. One day after the case was transferred to federal court on August 8th, CES staff used industrial magnets to wipe the back-up server hard drive, making all data on it unrecoverable. Once the internal emails of CES and KSU were obtained, it was easy to speculate on the officials’ motivations for such deliberate and rapid destruction of the records just after the lawsuit was filed.

Officials concealed voting system vulnerabilities

During the past fourteen months, CES/KSU officials have been discussing on email among themselves the severe vulnerabilities of the system, but concealing that alarming information from the public. KSU officials at CES and University Information Technology Services internally acknowledged that the CES main server, the hub of Georgia’s voting system, was “compromised,” contained “severe vulnerabilities,” allowed “malicious users” to gain access, and had dozens of “critical vulnerabilities” that put election programming and voter registration credentials at risk. Such damning descriptions were repeatedly made in officials’ internal emails that we obtained in an Open Records Request.² In these emails, they discussed their condemning analysis in the fall of 2016 in the run-up to the presidential election and again prior to the June 20th Sixth Congressional District

² <https://www.scribd.com/document/362955444/October-FOIA-responses-from-KSU-reordered-pages>

special election. This information was revealed in response to our Open Records Request received a few days ago.

For years, national experts in security of voting systems have warned that Georgia's electronic system is unreliable and should not be employed in its elections. Our lawsuit, *Curling v. Kemp*, alleges the noncompliant nature of the system and its significant deficiencies in meeting minimum statutory requirements.³ We detail material security flaws backed up by expert affidavits⁴ in the complaint filed in state court prior to transfer to federal court. The experts consistently testify that Georgia's system is not reliable for use in public elections, and they specifically warned Secretary Kemp after reports of system intrusions.⁵ However, the disclosures in the CES/KSU internal emails disclosed that the system is far more widely compromised and vulnerable than we assumed. In light of this new confirming information from those responsible for maintaining the CES system, election officials cannot responsibly use the electronic system for the current municipal elections. Those who do cannot legally certify the election outcomes, given the system's known vulnerabilities and noncompliance.

Officials have publicly maintained that Georgia's system is "safe," "secure," and protected from malicious actors despite the many warnings, admonitions, and testimony by the nations' experts that Georgia's equipment is insecure and unfit for use. Georgia's superficial pre-election equipment testing is little more than theatre meant to create the appearance of effective testing and security, but unfortunately it proves almost nothing. State officials in charge of the voting system have refused to publicly acknowledge the critical system flaws that they

³ <https://www.scribd.com/document/362956339/Second-Amended-Complaint-Curling-v-Kemp>

⁴ See Exhibits F, G, H, of 1st amended complaint
<https://www.scribd.com/document/355554359/CURLING-v-KEMP-Amended-Complaint>

⁵ <https://www.scribd.com/document/349999745/May-24-2017-Letter-to-SOS-Kemp-from-Computer-Experts>

discuss privately, as they continue to employ illegal systems. That is the fundamental reason for our lawsuit.

Compromised servers compromise the total voting system

Given the severe risks of corruption of the voting system programming that has resided on the compromised CES server for years, every DRE voting machine, optical scanner, GEMS server, GEMS database, ExpressPollbook, memory card, etc. must be considered compromised and unfit for use. It is almost impossible to disinfect the system from the potential malware to which it has likely been exposed for a long period of time. Field testing of the voting and tabulation equipment will not detect most malware. The system components simply cannot be used in compliance with the law and cannot produce a reliable result for election results certification.

Near-term remedies

Each election superintendent has the statutory duty to determine whether issues with the DRE system make it “impracticable for use,” and the superintendents are authorized to employ paper ballots when they make such a determination. It is clearly not appropriate or “practicable” to employ compromised and noncompliant voting equipment that violates state statutes.

As difficult as a mid-election change may be, continuing to use the compromised system can only make a bad situation worse, likely triggering numerous post-election legal challenges to the results by losing candidates and their supporters.

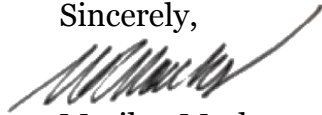
Summary

County and municipal officials and municipal candidates must not turn a blind eye to the flawed election being conducted, given the seriousness of these acknowledged vulnerabilities in the election system emanating from its source for programming—the CES compromised files. The admitted vulnerabilities of the servers that may have permitted corruption of the voting equipment are far more

pervasive and serious than even the experts imagined could be the case before the CES/KSU emails came to light. We urge you to take immediate responsible action to remedy this serious problem and to create a fair and certifiable municipal election in which the voters and candidates can have confidence.

We have attached an Appendix of related materials that may be useful to you and your colleagues as you consider the serious decisions before you. If you wish to discuss this issue, we are happy to hear from you and can introduce you to numerous voting systems experts standing ready to help.

Sincerely,

A handwritten signature in black ink, appearing to read 'Marilyn Marks', written in a cursive style.

Marilyn Marks

Executive Director, Coalition for Good Governance

CoalitionforGoodGovernance.org

Marilyn@USCGG.org

Appendix

1. May 2017 request of Secretary Kemp to re-examine the voting system. He has not done so:
<https://www.scribd.com/document/348665161/05-10-2017-Citizens-Letter-to-SOS-Kemp-re-voting-system-reexamination>
<https://www.scribd.com/document/348665000/5-17-17-Citizen-s-letter-to-SOS-Kemp-re-Voting-System>
2. Story of security failures prior to GA06 election
<https://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255>
3. Litigation hold letter issued to CES SOS
<https://www.scribd.com/document/362954849/7-10-17-Record-Retention-Letter-to-Defendants-Counsel>
4. News stories and two Georgia papers' op-eds re: records destruction
APNewsBreak: Georgia election server wiped after suit filed, by Frank Bajak | AP, October 26, 2017. <https://apnews.com/7d63dd986bd34e7286a14807f514aca4>.
Georgia election server wiped days after lawsuit, by Joe Uchill | The Hill, October 26, 2017. <http://thehill.com/policy/cybersecurity/357323-georgia-election-server-wiped-days-after-lawsuit>.
Kemp starts probe after data on Georgia election computer destroyed, by Greg Bluestein and Maya T. Prabhu | The Atlanta Journal-Constitution, October 26, 2017. <https://www.myajc.com/news/state--regional-govt--politics/ke...er-destroyed/YbX6G77vFqgEdqCCvB987O/politicallygeorgia.html>.
APNewsBreak: Q&A: Why wiping of Georgia elections server matters, by Frank Bajak | AP, October 26, 2017. <https://apnews.com/7d63dd986bd34e7286a14807f514aca4>.
Incompetence or a Cover-Up? — Georgia destroyed election data right after a lawsuit alleged its voting system might have been hacked, by Jeremy Stahl | Slate, October 27, 2017. *[A particularly useful article with a detailed timeline.]*
http://www.slate.com/articles/technology/future_tense/2017/10/georgia_destroyed_election_data_right_after_a_lawsuit_alleged_the_system.html
Georgia's voting system - Outrageous security lapse, Editorial | Savannah Morning News, Posted October 27, 2017.
<http://savannahnow.com/opinion/editorial/2017-10-27/editorial-georgia-s-voting-system-outrageous-security-lapse>
Georgia's election technology 'problem' is now a suspicious trash fire, By Dusty Nix | Ledger-Enquirer (Columbus), October 27, 2017 1:29 PM.
<http://www.ledgerenquirer.com/opinion/article181273691.html>