6th District Special Election Bulletin 14
June 16, 2017
Contact: Garland Favorito
(404) 664-4044

Georgia Election Officials Cover-up Critical Security Breach

ATLANTA GA – The person who breached the Kennesaw State University (KSU) Center for Election Systems (CES) that supports Georgia voting systems has finally been identified in an article from Kim Zetter published by Politico. Zetter confirmed that he was not a "hacker" but an internet security firm employee named Logan Lamb, who also was a cybersecurity researcher at the Oak Ridge National Laboratory in Tennessee. **Last August, Lamb independently decided to check on CES security** after nationwide reports of various breach attempts**.**

In his first interview, Lamb told Zetter he was browsing the CES public web site and **stumbled upon folders of voting system files that could be accessed to hack an election**. He ran a script that surprisingly downloaded 15 Gigs of data. The data included the voter registration database containing names, addresses and social security numbers for **6.7 million voters**. Lamb also noticed CES was using an out of date version of the DruPal content management system. The version has a major **security flaw** called "Drupageddon" that allows intruders to take control of a site.

Lamb contacted CES Executive Director Merle King about the breach and thought preventive measures would be taken but that is where things get bizarre. **King did not ensure all vulnerabilities were corrected and never notified the Secretary of State's Office (SOS)**. About March 1st, Lamb's colleague Chris Grayson found he could access the same files that Lamb did. Grayson confirmed the **Drupal flaw still existed** on the unencrypted portion of the site. He contacted a security instructor at KSU who contacted KSU's Information Security Office (UITS). They notified the state about March 2nd and prepared a security assessment on April 18th.

But it gets more bizarre. On April 27th **the SOS office claimed they did not have such a document** in response to VoterGa's Open Records Request (ORR). It asked for documents the SOS received from KSU in regards to a voting database breach on or about March 1. VoterGa obtained the UITS assessment on May 3rd with an ORR to KSU. But in the June 7th paper ballot lawsuit hearing, the **SOS legal counsel refused to acknowledge authenticity of the KSU security assessment!**

These newly revealed facts lead to some very disturbing conclusions:

- After being informed about a critical CES vulnerability in 2016, Merle King did not notify the SOS office and allowed it to continue unimpeded
- The SOS refused twice to recognize that KSUs security assessment exists
- The vulnerabilities may have been present at CES for a decade or more