May 24, 2017

The Honorable Brian Kemp
214 State Capitol
Atlanta, Georgia 30334

Dear Secretary Kemp,

On March 14th we sent a letter to you expressing grave concerns regarding the security of Georgia's voting systems and requesting transparency from your office concerning key questions about the reported breach at Kennesaw State University Center for Election Systems (KSU).

The FBI has reportedly closed its investigation into the breach at KSU and will not be pressing federal charges[1] but regrettably little more is known. We remain profoundly concerned about the security of Georgia's votes and the continued reliance on Diebold paperless touchscreen voting machines for upcoming elections.[2]

The FBI's decision not to press charges should not be mistaken for a confirmation that the voting systems are secure. The FBI's responsibility is to investigate and determine if evidence exists indicating that federal laws were broken. Just because the FBI concluded this hacker did not cross that line does not mean that any number of other, more sophisticated attackers could not or did not exploit the same vulnerability to plant malicious software that could be activated on command. Moreover, the FBI's statement should not be misinterpreted to conclude that KSU or the Georgia voting system do not have other security vulnerabilities that could be exploited by malicious actors to manipulate votes.

Any breach at KSU's Election Center must be treated as a national security issue with all seriousness and intensity. We urge you to engage the Department of Homeland Security and the US Computer Emergency Readiness Team (CERT) to conduct a full forensic investigation. We cannot ignore the very real possibility that foreign actors may be targeting our election infrastructure.

The FBI investigation lasted a mere few weeks. It's our understanding that this investigation was designed to determine whether criminal charges should be brought. However, a truly comprehensive, thorough and meaningful forensic computer security investigation likely would not be completed in just a few weeks, and it could take many months to know the extent of all vulnerabilities at KSU, if any have been exploited and if those exploits extended to the voting systems. Time and again cyber breaches are found to have been far more extensive than initially reported. When the breach at the Office of Personnel and Management was discovered in March of 2014 it was not disclosed to the public because officials concluded (incorrectly) that there was no loss of personal identifying information. The system was then reviewed by a private security

[1] Torres, Kristina, "Feds: "Security Researcher" behind KSU data breach broke no federal law," *Atlanta Journal Constitution,* March 31, 2017

[2] Diamont, Aaron, "KSU takes back seat in Georgia elections after server hack," *WSB-TV2 Atlanta News,* March 17, 2017

firm which determined in May (again incorrectly) that the system's security was sound.[3] One month later news reports surface warning that 25,000 individuals' personnel records have been compromised. A year later, that number had grown to over 21 million plus the fingerprints of 5.6 million employees.[4]

Problems reported during the April 18th special election have only escalated our concerns. According to news reports, an error occurred during the uploading of votes in Fulton County on election night.[5] Fulton's director of registration and elections, claimed that when a memory card was uploaded to transfer vote totals the operation failed and the system generated an error message that was "gobbledygook, just junk, just letters."[6] This sort of error message could be the result of a corrupted database and more investigation is needed.

While one cause of database corruption could be cyber intrusion which should not be ruled out, it is important to note that it was documented over ten years ago that the Diebold GEMS database used in Georgia is vulnerable to database corruption, especially if databases are run concurrently[7] as reportedly occurred in the recent special election.[8] This is because GEMS was built on Microsoft JETS database software, an outdated database which cannot be relied upon to provide accurate data.

According to Microsoft:

> "*When Microsoft JETS is used in a multi-user environment, multiple client processes are using file read, write, and locking operations on a shared database. Because multiple client processes are reading and writing to the same database and because JETS does not use a transaction log (as do the more advanced database systems, such as SQL Server),* ***it is not possible to reliably prevent any and all database corruption."***[9][Emphasis added.]

The voting system database stores the vote data. Corruption of the database could mean vote data, or vote counts, are lost. Because Georgia still relies on touchscreen voting machines that do not provide a paper ballot, if votes data is corrupted, it is possible that vote totals could be lost and without a physical paper ballot, there is no way to restore and correct the vote count.

This would be an excellent time to move with all expediency to replace Georgia's outdated voting system, to adopt paper ballot voting and implement robust manual post-election audits. The threat that foreign hackers might target the Dutch national elections caused the Netherlands

[3] "Timeline: What We Know about the OPM Breach," *NextGov.com, http://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/*

[4] Rosenfeld, Everett, "Office of Personnel and Management: 5.6 million estimated to have fingerprints stolen in breach," *CNBC,* September 23, 2015

[5] Kass, Arielle, "'Rare error' delays Fulton County vote count in 6th district race," *Atlanta Journal Constitution,* April 19, 2017

[6] *Ibid*.

[7] Hoke, Candice, Ryan, Thomas, "GEMS Tabulation Database Design Issues in Relation to Voting System Certification Standards," https://www.usenix.org/legacy/event/evt07/tech/full_papers/ryan/ryan.pdf

[8] Kass, Arielle, "'Rare error' delays Fulton County vote count in 6th district race," *Atlanta Journal Constitution,* April 19, 2017

[9] How to Troubleshoot and to Repair a Damaged Access 2002 or Later Database, (Rev. 6.1 2006) at http://support.microsoft.com/default.aspx?scid=kb;en-us;283849

to cancel all electronic voting and hold its March elections on paper ballots. The U.S. has not responded to the threat of foreign hacking with the same accountability and speed. The former director of U.S, national intelligence James Clapper recently told Congress that foreign hackers will continue to attack and we should expect them in the 2018 and 2020 elections.[10]

We believe this is a profoundly serious national security issue. We stand ready to help you any way we can to help protect our democratic process and regain the confidence of voters.

Sincerely,

Dr. Richard DeMillo
Charlotte B, and Roger C. Warren Professor of Computing
Georgia Tech

Dr. Andrew W. Appel
Eugene Higgins Professor of Computer Science,
Princeton University

Dr. Duncan Buell
Professor, Department of Computer Science & Engineering, NCR Chair of Computer Science & Engineering,
University of South Carolina

Dr. David L. Dill
Professor of Computer Science,
Stanford University

Dr. Michael Fischer
Professor of Computer Science,
Yale University

Dr. J. Alex Halderman
Professor, Computer Science and Engineering
Director, Center for Computer Security and Society
University of Michigan

Candice Hoke
Co-Director, Center for Cybersecurity & Privacy Protection and Professor of Law,
Cleveland State University

Harri Hursti
Chief Technology Officer and co-founder, Zyptonite, and founding partner, Nordic Innovation Labs.

Dr. David Jefferson
Lawrence Livermore National Laboratory

Dr. Joseph Kiniry
Principal Investigator, Galois
Principled CEO and Chief Scientist,
Free & Fair

Dr. Ronald L. Rivest
MIT Institute Professor

[10] Ng, Alfred, "Ex-intel chief James Clapper warns of more Russian hacks," *CNET,* May 8, 2017

Dr. John E. Savage
An Wang Professor of Computer Science,
Brown University

Dr. Barbara Simons
IBM Research (retired),
former President Association for Computing Machinery (ACM)

Dr. Philip Stark
Associate Dean, Division of Mathematics and Physical Sciences,
University of California, Berkeley

Affiliations are for identification purposes only, they do not imply institutional endorsements.