March 14, 2017

The Honorable Brian Kemp
214 State Capitol
Atlanta, Georgia 30334

Dear Secretary Kemp,

On March 3rd it was reported that the Federal Bureau of Investigations is conducting a criminal investigation into an alleged cyber attack of the Kennesaw State University Center for Election Systems. According to the KSU Center for Election Systems' website, "the Secretary of State authorized KSU to create a Center for Election Systems, dedicated to assisting with the deployment of the Direct Record Electronic (DRE) voting technology and providing ongoing support."[1] The Center is responsible for ensuring the integrity of the voting systems and developing and implementing security procedures for the election management software installed in all county election offices and voting systems.

The Center has access to most if not all voting systems and software used in Georgia. It also is responsible for programming these systems and accessing and validating the software on these systems. It is our understanding that the Center also programs and populates with voter records the electronic poll books used in polling places statewide. A security breach at the Center could have dire security consequences for the integrity of the technology and all elections carried out in Georgia.

In order for citizens to have faith and confidence in their elections, transparency is crucial, including about events such as the KSU breach, and its extent and severity. While we understand that this investigation is ongoing and that it will take time for the full picture to emerge, we request that you be as forthcoming and transparent as possible regarding critical information about the breach and the investigation, as such leadership not only will be respected in Georgia but also emulated in other states where such a breach could occur. We expect that you are already pursuing questions such as the following, regarding the breach, and trust that you will make public the results of such inquiry:

1. Can you estimate when the attacker breached KSU's system?
2. How did the attacker breach KSU's system?
3. How was the breach discovered?
4. Which files were accessed?
5. Were any files accessed that related to software or "hashes" for the voting machines?
6. Is there any evidence that files were modified? If so, which files?
7. Had KSU begun ballot builds for the upcoming special election?
8. To whom are these attacks being attributed? Could this be an insider attack? Has the FBI identified any suspects or persons of interest?

---

[1] http://elections.kennesaw.edu/about/history.php

9. Has the FBI examined removable media for the possibility of implanted malware?
10. Has the FBI examined the hash or verification program for tampering?
11. What mitigations are planned for the near- and long-term?

In any state an attack on a vendor providing software and system support with such far-reaching responsibilities would be devastating. This situation is especially fragile, because of the reliance on DRE voting machines that do not provide an independent paper record of verified voter intent. KSU has instead sought to verify the validity of the software on the voting machines by running a hash program on all machines before and after elections in an effort to confirm that the software has not been altered. However, if KSU's election programming were compromised, it is also possible that the verification program could have been modified to affirm that the software is correct, even if it were not. This is a risk of using software to check the correctness of software.

Of course all Georgia elections are important. This month and next include special elections as well. If these upcoming elections are to be run on DREs and e-pollbooks that are maintained and programmed by KSU while the KSU Center for Election Systems is itself the subject of an ongoing criminal investigation, it can raise deep concerns. And today's cyber risk climate is not likely to improve any time soon.

We urge you to provide Georgia's citizens with information they need to confirm before going to vote that their name will appear correctly on the voter rolls, as well as back-up printed voter lists in case anomalies appear. Most importantly, we urge you to act with all haste to move Georgia to a system of voter-verified paper ballots and to conduct post-election manual audits of election results going forward to provide integrity and transparency to all of Georgia's elections. We would be strongly supportive of such efforts and would be willing to help in any way we can.

Sincerely,

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. Larry Diamond
Senior Fellow, Hoover Institute and
Freeman Spogli Institute, Stanford University

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

Dr. Joseph Lorenzo Hall
Chief Technologist,
Center for Democracy & Technology

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

Dr. Douglas W. Jones
Department of Computer Science
University of Iowa

Dr. Justin Moore
Software Engineer, Google

Dr. Ronald L. Rivest
MIT Institute Professor

Bruce Schneier
Fellow and lecturer
Harvard Kennedy School of Government

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

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

Dr. David Jefferson
Lawrence Livermore National Laboratory

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

Dr. Peter G. Neumann
Senior Principal Scientist, SRI International
Computer Science Lab, and moderator of the
ACM Risks Forum

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. Vanessa Teague
Department of Computing & Information
systems, University of Melbourne

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