January 7, 2019

The Honorable Robyn Crittenden
Secretary of State Elect Brad Raffensperger
Rep. Barry Fleming
Members of the SAFE Commission
214 State Capitol
Atlanta, Georgia 30334 (via e-mail)

Dear Secretary Crittenden, Secretary Elect Raffensperger, and SAFE Commission Members:

We write to urge you to follow the advice of election security experts nationwide, including the National Academies of Sciences, the Verified Voting Foundation, Freedomworks, the National Election Defense Coalition, cyber security expert and Commission member Professor Wenke Lee, and the many states that are abandoning vulnerable touchscreen electronic voting machines in favor of hand-marked paper ballots as the best method for recording votes in public elections.

Our strong recommendation is to reject computerized ballot marking devices (BMDs) as an option for Georgia's voting system, except when needed to accommodate voters with disabilities that prevent them from hand-marking paper ballots. Hand-marked paper ballots, scanned by modern optical scanners and used in conjunction with risk-limiting post-election audits of election results, should be the standard balloting method statewide.

Although they are expensive and complex devices, computerized ballot markers perform a relatively simple function: recording voter intent on a paper ballot. Since there are no objective, quantitative studies of their benefits, acquiring BMDs for widespread use risks burdening Georgia taxpayers with unnecessary costs. Furthermore, BMDs share the pervasive security vulnerabilities found in all electronic voting systems, including the insecure, paperless DREs in current use statewide. These reasons alone should disqualify BMDs from widespread use in Georgia's elections, especially since there is a better alternative.

Hand-marked paper ballots constitute a safer and less expensive method of casting votes. Hand-marked paper ballots offer better voter verification than can be achieved with a computerized interface. A paper ballot that is indelibly marked by hand and physically secured from the moment of casting is the most reliable record of voter intent. A hand-marked paper ballot is the only kind of record not vulnerable to software errors, configuration errors, or hacking.

The SAFE Commission has heard testimony about voter errors in marking paper ballots and the susceptibility of paper ballots to tampering or theft. No method of balloting is perfect, but vulnerabilities in computerized marking devices, if exploited by hackers or unchecked by bad system designs, raise the specter of large-scale, jurisdiction-wide failures that change election outcomes. For example, with hand-marked paper ballots, voters are responsible only for their own mistakes. On the other hand, voters who use BMDs are responsible not only for

their own mistakes but also for catching and correcting errors or alterations made by a BMD which marks ballots for hundreds of voters. For this reason, well-designed hand-marked paper ballots combined with risk-limiting post-election tabulation audits is the gold standard for ensuring that reported election results accurately reflect the will of the people.

Voter verification of a BMD-market ballot is the principle means of guarding against software errors that alter ballot choices. Many BMDs present a ballot summary card to the voter for verification. The 2018 National Academies of Science, Engineering and Medicine Consensus Report *Securing the Votes: Protecting American Democracy*, which represents the nation's best scientific understanding of election security and integrity, states: "Unless a voter takes notes while voting, BMDs that print only selections with abbreviated names/descriptions of the contests are virtually unusable for verifying voter intent." Although advocates of touchscreen ballot marking devices claim that the human readable text ballot summary cards are "voter verifiable," the contrary is true: voter verified summary cards that contain errors (whether induced by hacking or by design flaws) are likely to be mistakenly cast, making a valid audit impossible. A post-election audit requires a valid source document, either marked directly by the voter or voter verified. Since voter verification of printed ballot summary cards (the source document) is sporadic and unreliable, elections conducted with most ballot marking devices are unauditable.

While you may have been told that touchscreen systems are more "modern" devices, many of your peers and most election security experts have found this appeal to be based on a mistaken view that the voting public will naively accept new technology as a "step forward." We are intimately familiar with the hidden costs, risks, and complexity of these new technologies. We can assure you there is objective scientific and technical evidence supporting the accuracy of traditional, easily implemented scanned and audited hand-marked paper ballot systems. We urge you to recommend such a system as the safest, most cost-effective, and transparent way of conducting future elections.

If we can be of help in providing more information, we hope you will feel free to call upon us.

Sincerely,

Dr. Mustaque Ahamad
Professor of Computer Science,
Georgia Institute of Technology

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

Dr. David A. Bader, Professor
Chair, School of Computational Science and Engineering
College of Computing
Georgia Institute of Technology

Matthew Bernhard
University of Michigan
Verified Voting

Dr. Matt Blaze
McDevitt Chair in Computer Science and Law
Georgetown University

Dr. Duncan Buell
NCR Professor of Computer Science and Engineering
Dept. of Computer Science and Engineering
University of South Carolina

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

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

David L. Dill
Donald E. Knuth Professor, Emeritus, in the School of Engineering and Professor of Computer Science, Stanford University
Founder of VerifiedVoting.org

Dr. Michael Fischer
Professor of Computer Science
Yale University

Adam Ghetti
Founder / CTO
Ionic Security Inc.

Susan Greenhalgh
Policy Director
National Election Defense Coalition

Dr. Candice Hoke
Founding Co-Director, Center for Cybersecurity & Privacy Protection
C|M Law, Cleveland State University

Harri Hursti
Security Researcher
Nordic Innovation Labs

Dr. David Jefferson
Lawrence Livermore National Laboratory

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

Dr. Justin Moore
Software Engineer
Google

Dr. Peter G. Neumann
Chief Scientist
SRI International Computer Science Lab
Moderator of the ACM Risks Forum

Dr. Ronald L. Rivest
Institute Professor
MIT

Dr. Aviel D. Rubin
Professor of Computer Science
Johns Hopkins University

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

Dr. Barbara Simons
IBM Research (Retired)
Former President, Association for Computing Machinery

Dr. Eugene H. Spafford
Professor
Purdue university

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.