Exhibit A

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

JILL STEIN, RANDALL REITZ, ROBIN HOWE, SHANNON KNIGHT, EMILY COOK, and KIMBERLY KUPKA,

Plaintiffs,

v.

PEDRO A. CORTÉS, *in his official capacity as Secretary of the Commonwealth;* and JONATHAN MARKS, *in his official capacity as Commissioner of the Bureau of Commissions, Elections, and Legislation,*

Defendants.

No. 16-CV-6287 (PD)

DECLARATION OF CANDICE HOKE

I, CANDICE HOKE, declare under penalty of perjury:

1. My name is Candice Hoke. I am the Founding Co-Director of the Center for Cybersecurity & Privacy Protection and a Professor of Law Emerita at Cleveland State University, Cleveland, Ohio. I reside in Pittsburgh, PA, and am registered to vote in Pennsylvania.

2. I hold a Master's of Science in Information Security Policy and Management from Carnegie Mellon University and a J.D. from Yale Law School. I have worked as a Cybersecurity Engineer as a member of the Cyber Risk & Resilience Team in the CERT Division of the Software Engineering Institute of Carnegie Mellon University.

3. My research focuses on election cybersecurity, cyber risk assessment, and data privacy. My published work and teaching include attention to the regulatory systems that govern electronic voting. I have testified before Congress on the importance of post-election auditing. I also have authored published works on election forensics, including a guide for

election officials and their lawyers that the American Bar Association distributed in 2008 free of charge to all members of the Section on State and Local Government Law. In the summer of 2016, cybersecurity staff in the U.S. Department of Homeland Security requested my assistance with election cybersecurity problems, which I provided pro bono.

4. I founded and directed the Center for Election Integrity, located at Cleveland State University, which focused on improving election administration throughout the nation, and specifically worked on the discovery and effective management of security vulnerabilities present in deployed voting equipment.

5. I have reviewed the Directive issued by Acting Secretary of State Robert Torres, dated February 9, 2008, regarding the purchase of new voting machines. While it is a step forward and implicitly recognizes that paper records are the means for correcting the capacity for software-based, all-electronic voting machines to modify votes and vote totals in largely undetectable ways, the Directive does not go nearly far enough in correcting the current threats to voting and electoral integrity. The Directive does not reduce the existing vulnerabilities, or augment the capacity for auditing and assessment of hacking and remote intrusion, that could render voting merely illusory in many Pennsylvania counties.

6. Secretary Torres did not decertify (and thus render unusable) all-electronic voting systems, including those aged, deeply flawed systems that are still used in the two most populous counties in the Commonwealth. These counties, and most of the others that deploy all-electronic voting systems, have been using them for over a decade despite the numerous, serious security (and therefore, potential vote and tabulation accuracy) defects in those machines. These defects have been documented in definitive research from the most respected computer security experts nationally, and were a focus of earlier declarations by me and other experts when this lawsuit was originally filed.

7. The Directive does not require henceforth the use of voting machines with voter-verified paper ballots or some type of paper records. Instead, it merely directs counties to

purchase voting systems that use some type of paper record whenever they next make voting machine purchases, if at all.

8. The Directive omits to impose a deadline for counties to transition from insecure and unauditable voting systems to more secure, auditable voting systems. Given that in statewide races the votes from all counties are accumulated to produce statewide totals, the lack of a clearly demarcated date for all counties to use secure, paper-based, auditable voting continues to undermine the security and accuracy of the entire Commonwealth's vote totals. Thus, the State's decisions with regard to the most insecure, all-electronic voting systems in some counties actually impact the voting rights of the entire Commonwealth citizenry. The Directive provides no date by which Pennsylvania voters throughout the State will have guaranteed access to cast their votes using voter-verified paper ballots to provide a check on insecure, hackable software in the voting systems and county election offices.

9. The Directive also omits clarity that those counties that do replace or upgrade their voting systems must select a paper-ballot system rather than adopt a "toilet-paper," heat-sensitive (and easily deteriorating) printout from an all-electronic DRE machine (hereafter "DRE"). The Affidavit of Daniel Lopresti, dated December 2, 2016, at ECF No. 11, correctly presents to the Court the definitive research findings from many respected studies that conclude paper printouts from DRE machines are no more reliable than the all-electronic voting machines' electronic totals. If a DRE machine is broken, compromised, or hacked, the paper printouts from the machine (that supposedly reflect the votes that were cast on the machine) can be false or falsified. This capacity to falsify votes cannot occur easily when voters mark paper ballots, and certainly not in a wholesale manner as is achievable in software hacks. For disabled voters, several options are available for "ballot marking devices" that will mark a ballot for the voter to review and verify before it is placed in the cast vote containers.

10. While an optical scan tabulation machine can be hacked to produce false counts of paper ballots, a post-election statistical audit can catch these covert or remote efforts, and allow for the election officials to produce authentic, provable totals of the vote because they have the

voter-marked paper ballots that can be hand-counted, or even re-tabulated with a provably "clean" scanner. When combined with sound auditing practices, these paper ballot voting options thus allow election officials and the Commonwealth to assure the public and themselves that voting rights are fulfilled and protected, and that hackers have not modified the totals.

11. Given the ease and myriad ways of covertly modifying the software of currently deployed all-electronic DRE systems that the Directive continues to authorize for voting in Pennsylvania and Federal elections, the counties and State cannot produce reliable evidence of what those voters' intent was, nor of the election totals that are based on votes cast.

12. That the Commonwealth continues to permit deployment of these antiquated voting systems functions as an open invitation to routine hackers, criminal syndicates, and hostile nation-state adversaries to engage in nefarious intrusions in Pennsylvania elections. Our counties are not prepared to defend from such activity, which heightens the importance of using secure voting systems that support vote auditing and correction in case of remote hacks.

13. I have also reviewed Defendants' papers submitted in support of their motion to dismiss, filed on February 9, 2018. Defendants oppose any type of forensic evaluation of the computers used in past elections, whether for election management (creation of ballots, tabulation and reporting), or the voting devices themselves. A forensic evaluation of a sample of the election management computers and voting machines could include assessments of whether they were affected by attackers, such as by modified program files, the presence of malware, and signs of remote intrusions.

14. While the best forensic evaluations are conducted close in time to the events in question, a forensic evaluation in the near future by qualified experts is not doomed to failure or inherently a waste of time. Repeatedly, law enforcement teams have been able to resurrect electronic data even from years previously to reconstruct electronic trails and events that can support successful prosecutions. But without voter-marked paper ballots, the Commonwealth

is unable to conduct valid recounts, and must expect that its voters and candidates will need to rely on forensic evaluations to assess and attempt to validate election totals.

15. If the entire Commonwealth used paper ballots in its voting, as many other States have already chosen to do (combined with the recounts and quality-assurance auditing that are thereby enabled), the reasons for any type of forensic evaluation of election computers would plummet. The Commonwealth's voters, candidates, and political parties, as well as its election officials, would have the capacity to rapidly achieve clarity and high, well-justified confidence in the election results that are produced. Hacking into the election computers to change votes could be identified and corrected via routine auditing of the paper ballots, significantly reducing the incentive for hacking. Any who reviewed that election evidence would be able to discern the accuracy of the vote totals, county by county and statewide, and thus perceive that the Commonwealth had provided and protected voting rights. This type of election assessment and conclusion is not possible with all-electronic voting systems-- the systems that the recent Directive fails to eliminate.

Dated: February 23, 2018
Pittsburgh, PA

Candice Hoke

Founding Co-Director, Center for Cybersecurity & Privacy Protection