AFFIDAVIT OF S. CANDICE HOKE

I, S. Candice Hoke, duly sworn, depose and say the following under penalty of perjury:

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

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 on the discovery and effective management of security vulnerabilities present in deployed voting equipment.

5. When Cuyahoga County, one of the largest election jurisdictions in the nation, first launched its e-voting system and suffered a major election disaster in which every technical and management system failed (May 2006), the Cuyahoga County Board of Elections and the County Commission jointly appointed me to a 3-person investigatory panel to ascertain the causes and cures. In that capacity, I worked to secure a forensics review of the absentee ballot scanners that intermittently had miscounted ballots, and hired and supervised investigatory

staff, leading the technical team in its overall assessment of operational and software election security. I was the major author of the Final Report that included over 300 action recommendations for improving the election process and its electronic voting systems.

6. After the Cuyahoga Election Review Panel submitted its report and recommendations, including the forensics evaluation, the same public bodies then appointed the Center for Election Integrity (of which I was the Director) to serve as Public Monitor of Cuyahoga Election Reform. I then worked for the next two years in that role, and was closely involved with the ongoing assessment and improvement of voting system security in Cuyahoga County (2006-08). I observed and documented in written reports various security vulnerabilities in actual elections operations, and violations of security policies. I was also involved in voting system procurement decisions when the County decided to replace its DRE precinct systems and move to optical scan systems with post-election auditing after every election.

7. While I was living in Ohio, I also served within the election system as a supervising poll worker; as a "roving" election technology trouble-shooter for many voting locations; as a voter registration problem-solver; and as a consultant to the Ohio Secretary of State's office on election management and improvement, including on voting technology issues.

8. In my academic capacity I have published peer-reviewed research that analyzes the security of electronic voting systems currently deployed in Pennsylvania, Ohio, California, and many other States. I was part of a team of experts commissioned by the California Secretary of State to conduct a "Top-to-Bottom Review" of that state's voting systems, specifically serving as a Research Team Leader for a portion of the Diebold study. I also served as a pro bono consultant to the Ohio Secretary of State in structuring that voting system security study.

The DRE Machines Used in Pennsylvania Are Vulnerable

9. All of the direct recording electronic (DREs) voting machines that Pennsylvania deployed in 2016 were designed to use software components that have been out of date for more than a decade. As such, they are pervaded with well-documented operational reliability and security deficiencies that can be easily yet covertly exploited in ways that can cause great harm to important data and systems.

10. All DRE voting systems offer the opportunity for covert tampering with memory media in ways that can lead to the central tabulator software or the election management system (EMS) to be infected with a virus or other malware that can lead to false vote counts. Because many counties outsource election services to vendors -- including for creating the electronic ballots and configuring the EMS database for tallying votes and for programming, testing, or delivering the DRE units to polling location—a wealth of opportunities exist for tampering with the election system to change the behavior of the software in ways that can cause them to deliberately miscount.

11. DRE systems currently deployed in Pennsylvania use antiquated and unreliable memory media to record votes. The vote aggregation methods among multiple DRE units at a precinct often confuse poll workers, and has not infrequently led to some memory cartridges not being tabulated or returned to the election office in a timely manner. Fortunately, some vendors of some of the voting systems used in Pennsylvania designed their systems to alert election officials when any of the DRE memory media are missing from the tabulations, so that the officials can seek out the location of that missing media and record the votes. But other DRE systems deployed in the Commonwealth lack that essential feature and thus render it exceptionally easy to miss some votes and produce inaccurate vote tallies.

12. The antiquated DRE touchscreens have been deployed well past their recommended life cycle, and not surprisingly, are losing their ability to respond accurately to voters'

selections. This problem can result in "vote flipping" between candidates. DRE touchscreens can also be misprogrammed - deliberately or accidentally—in ways that can cause the votes not to track accurately. Logic and Accuracy (L & A testing) in advance of elections is supposed to catch and provide the opportunity to correct such errors before voters cast their ballots. But few election jurisdictions use the depth and scope of L & A testing required to assure that their DRE systems have not been misprogrammed or have "rogue code" planted on them. Malware and code designed to mis-record voters' choices by changing votes to count for other candidates can be designed to activate only at a certain time after the L & A testing, and there are many other ways for cheating code to avoid being detected by L&A tests.

13. The DREs cannot function without an EMS configuring the ballot and generating the "instructions" that the DRE will use for presenting the ballot to the voter and recording the cast votes. Hence, the EMS and DRE vulnerabilities - both as to security and reliability -- are interrelated and impact one another.

14. As examples of how normal functioning of a poorly designed EMS can lead to the vote tabulation database "dumping" data - i.e., votes -- or "corrupting" that data, I would submit the experience of Cuyahoga County, Ohio. Because I served as the Project Director of the Public Monitor of Cuyahoga Election Reform, and had convened a technical team with access to tabulation records, we were able to publicly document that in the May 2006 primary, the GEMS database grew beyond the capacity that software could handle. Concretely, this meant that as DRE vote media and the scanned absentee ballot batches were uploaded to the GEMS server, GEMS covertly - without notice to officials-- dumped some of that data because its Microsoft JET / Access database foundation was not able to manage that amount of data. As a result, hundreds of votes in one county alone were not recorded and recounts determined that some previously announced winners actually had not won.

15. In the November general election of 2006, while preparing for the election and then on election night during the tabulations, the GEMS servers were repeatedly crashing. As Monitor, we staffed the tabulation server room and noted each time the server crashed; the security plan also required that an official record be made of each and every server crash, with its time and operator input when it occurred. Because we knew that servers crashing during tabulations could cause data corruption, we sought a forensic review of the database to ascertain whether vote data integrity had been preserved. We documented a number of indicators of data corruption, including database table element entries that missed their date/time stamps of when the information was entered; other tabulation entries' date/time stamps were marked "January 1, 1970," which is the epoch (zero- point) of UNIX time—rather than carrying the 2006 date and time. Finally, vote totals in two separate database tables held different values for the candidates' results, differing by hundreds of votes.

A Fornsic Evaluation of the DREs Is the Only Way to Determine the Accuracy of the Vote

16. Given (a) the multiple available pathways for inserting malware or code that can cause vote flipping or miscounts; (b) the clear existence and motivation of numerous skilled and motivated hackers, including from nation-state adversaries; (c) the unreliability of the systems owing to their age and defective software designs, and (d) repeated crashing during pre-election and election tabulations, a recount that includes a forensics assessment of the EMS and at least a random selection of the DREs and associated components is necessary to ascertain whether the reported tallies are accurate.

17. Voting system experts who have no financial relationship to the vendors or their contracts, and who have developed expertise in these systems deployed in the Commonwealth can efficiently conduct forensics reviews in a targeted manner, focusing on the main frailties in these systems. For instance, in one 2-hour session in Cuyahoga County, one Monitor staff database examiner was able to document all the irregularities mentioned in paragraph 15,

supra. While most forensics assessments would not proceed this quickly, and investigating and correcting for the anomalies consumed some additional time, valuable information can be obtained in a matter of hours regarding whether the system performed as expected and required. . Forensics reviews are the only means to check whether all these functions are performed accurately for all-electronic DRE systems.

18. One of the additional values of an independent forensics review is that it allows the public and public authorities to obtain essential information relevant to whether and when they choose to replace the dilapidated voting systems. In Cuyahoga County, for instance, the officials made a decision to replace the GEMS-and-DRE system because it proved to be too unreliable and difficult to manage in a secure manner. In barely 1.5 years after our reports documenting these operational and the software architectural issues (that the vendor had hidden and that could not be fixed without a wholesale re-architecting of the software), Cuyahoga County chose to replace its voting system with a more reliable and accurate option.

19. Although I have personally listened to fears of election and other public officials that they will be accused of wrongdoing, or that the public will blame them personally for any problems that are discovered in a forensics review of election systems, or that the voting public will refuse to participate in voting if they learn of technical and other deficiencies in their election equipment, I would like to relate what occurred in Cuyahoga County. The May 2006 Federal primary election vote tally reports proved to be unreliable and inaccurate, in at least some races, and serious public questions were raised about the adequacy of the voting technologies. Instead of a superficial fix, our County's appointed independent investigatory team endeavored to figure out everything that had gone wrong, technically and managerially, and to disclose everything in public reports. We sought to assure the public that their voting rights were protected and that their choices would be accurately recorded and tabulated at least in future elections. We asked for the public's participation via public hearings on their

experiences and concerns, and retooled poll worker recruitment and training to ensure that fewer errors could occur at the polls. The public responded vigorously, attending standing room only public hearings and producing a large number of new volunteers to work as poll worker and in other roles. That fall, for the general election, our voting participation rates rose instead of falling and we had scores of new citizens involved in the election system in a variety of roles, all proving that transparency on voting problems can produce public energy and dedication to participate as well as help improve the election system.

20. As a voting systems and election administration specialist, and as cyber risk expert, I am concerned that hackers and other miscreants have learned that Pennsylvania has erected a series of legal obstacles that generally inhibit checking into the integrity of county election tabulations. Thinking from the security perspective, this legal cover basically provides a neon sign to motivated hackers both domestically and abroad, saying "*Come Hack Here; we won't be checking.*" Hackers seek valuable and preferably unprotected targets, and those who have been documented by Federal authorities to have interfered in this election cycle would have been highly motivated to try to probe and impact Pennsylvania's systems. As an election management and security specialist, I recommend that Pennsylvania clearly establish that its elections are not open to any motivated hacker and that the Commonwealth assures that accurate voting tallies are generated without incursion by unauthorized others.

This affidavit was executed on the 2nd day of December, 2016, in Cleveland, Ohio.

S. Candice Hoke

Sworn before me this 2nd day of December, 2016.

Notary Public

My Commission expires: KENNETH J. KOWALSKI, Atty. NOTARY PUBLIC • STATE OF OHIO My commission has no expiration date Section 147.03 O.R.C.