AFFIDAVIT OF POORVI L. VORA

POORVI L. VORA, being duly sworn, deposes and says the following under penalty of perjury:

1. My name is Poorvi L. Vora. I am a Professor of Computer Science at The George Washington University (GW) in Washington, DC. I submit this Affidavit in support of Jill Stein's Petition for a hand recount of all ballots in Michigan.
2. I have Ph. D. and Master's degrees in Electrical Engineering from North Carolina State University, Raleigh, NC, a Master's degree in Mathematics from Cornell University, and a Bachelor's degree in Electrical and Electronics Engineering from the Indian Institute of Technology, Bombay, India. My CV is attached as Exhibit A.
3. My research in the last dozen or so years has focused on computer security and privacy, with a special focus on secure electronic voting systems.
4. I have published peer-reviewed research on the design of secure end-to-end-verifiable (E2E-V) voting systems which are software-independent voting systems that enable voters and observers to perform especially powerful election audits. I have also helped the National Institute of Standards and Technology develop definitions of E2E-V system properties.
5. With my students and collaborators, I contributed to the design and deployment of an E2E-V voting system called Scantegrity in the municipal elections of the City of Takoma Park, MD in 2009 and 2011. 2009 marked the first time an E2E-V system was used in a government election. We also designed accessible and absentee voting variants of Scantegrity, which were used by Takoma Park in 2011.

6. I was an invited contributor to the Open Vote Foundation study: “The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study” which concluded that secure internet voting is not possible at this time.
7. I have recently been providing public comment in person at meetings of the State Board of Elections in Maryland to urge Maryland to carry out an election audit using its voter-verified paper ballots.
8. I have been on program committees of several conferences and review panels for National Science Foundation research awards. I have been an Associate Editor for the IEEE Transactions on Information Forensics and Security, and a Guest Editor for the IEEE Transactions on Information Forensics and Security special issue on electronic voting in December 2009.
9. I regularly teach a course on Cryptography (mathematical techniques that enhance computer security and are used in the design of secure voting systems and secure electronic commerce) for undergraduate and graduate students. I also often teach a more general course on Computer Security, and a course on Advanced Cryptography.
10. It is, of course, important for a voting system to produce the correct tallies. The system —whether paper-based, or electronic, or a combination thereof—should also be designed to enable voters and observers to verify that it produced the correct tallies once the election is over.
11. When votes are cast on paper ballots which are hand counted, the verification is performed through public observation of the counting process. When counts are computed using inherently unobservable software-based systems, the verification of the tallies has not always been possible.

12. Software-based voting systems are very complex and may consist of hundreds of thousands of lines of code[1].

13. It is hence not possible to find all bugs in voting system software; nor is it possible to completely characterize its behavior in all scenarios. For the same reasons, it is not possible to determine with certainty the absence of malicious software hiding within what might appear to be many thousands of lines of legitimate software code. Additionally, it is not possible to confirm with certainty that the code running on the machines during the election is the code that was examined before the election.

14. One approach to dealing with this fundamental challenge of verifying the outcome of software-based voting systems is the notion of *software-independence*,[2][3] as described by Rivest and Wack. A *software-independent* voting system is one in which an undetected change in the voting system software will not cause an undetected change in election outcome. Note that a software-independent system is not one that does not use software. It is a system that has a means of verifying the election outcome, independent of the software that computed it (because that software could have bugs and malicious code that have not been detected).

15. One way of achieving software-independence is through the use of voter-verified paper records (VVPRs) securely stored and used to audit the election after it is completed. VVPRs may consist of (a) printouts from Direct-Recording Electronic (DRE) machines,

[1] For example, there were“670,000 lines of code, encompassing twelve programming languages and five hardware platforms” in a study of the ES&S system, which includes a version of the Model 100 scanner used in some Wisconsin jurisdictions this year.   “EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing”, Final report, December 2007, http://www.patrickmcdaniel.org/pubs/everest.pdf (hereinafter the “Everest Study”).

[2] Ronald L. Rivest and John P. Wack. “On the notion of `‘software independence’ in voting systems.” (2006), https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf

[3] Ronald L. Rivest. “On the notion of `software independence’ in voting systems.” *Philosophical Transactions of The Royal Society A* 366,1881 (2008) pp. 3759--3767.

verifiable by voters as correctly representing their votes or (b) paper ballots completed by voters and fed into optical scanners that tabulate the votes.

16. As a general principle, both optical scanners and DREs are computers running software and hence are vulnerable to the same problems—bugs, malware, intentional alterations, etc.—as all software.[4]

17. Hence the mere act of recording a vote on paper is not sufficient for software independence. The securely stored paper records need to be examined to ensure that they are consistent with the election outcomes declared by the voting system software. If they are not examined, any unintentional software bugs, intentional alterations to the vote or to the tally, or procedural errors leading to an incorrect election outcome will not be detected.

18. A voter using an optical scanner marks a paper ballot and feeds it into the scanner. The voter does not know if it has read her votes correctly.

19. The scanner uses light measurements to determine what ballot positions have marks on them, or to take a digital image. It may store the images thus generated as ballot scans. While the scans do originate through a physical process, and may be visually represented as images on a computer screen, they are not like photographs. They are computer data, stored as ones and zeroes and handled by computer software. As a general principle, though the specifics may vary with the specific op-scan system, they can be deleted,

[4] According to the Everest Study, "… although they do not appear the same as your typical desktop or laptop computer, all the components of the ES&S system are fully programmable computers capable of running arbitrary software stored in easily modifiable memory. Therefore use of the term "firmware" to refer to the software controlling the hardware components of the ES&S system is somewhat misleading. The code running on the iVotronic [DRE] or Model 100 [optical scanner] is in no way less susceptible to bugs, tampering, or co-option than any other part of the Unity system." *See* Everest Study, *supra* n. 1.

replaced or tampered with like any other computer data. Additionally, the recording process itself can be erroneous.

20. Of particular concern this year are the many undervotes for the Presidential race in Michigan: there are 75,335 fewer votes recorded for President than there were ballots cast. This is a 50% increase in the number of undervotes from 2012; the corresponding increase in number of voters is smaller than 2%! While there could be multiple explanations for this large increase in the number of undervotes, undervotes can be caused due to scanner error or intentional alteration of scan data or the votes the data represent. Only a manual examination of the ballots can definitively determine whether all the undervotes are truly undervotes. This is important because the number of undervotes is about 7 times the margin of the race.

21. Once the scanner has obtained the scan data, it uses instructions regarding the order and position of the various contests and options to determine the votes on a ballot. These ballot programming instructions are delivered, shortly before every election, generally through a removable memory device.

22. A scanner may misinterpret a vote for various reasons: a voter may not have marked the oval as expected to—she may check the oval or circle the candidate's name; a voter may make very light marks on the ballot that are not detected; some optical scanners may not detect red ink[5]; ballot programming errors or intentional hacking can lead to votes being swapped among candidates. Newer scanners use more sophisticated techniques to deal with light marks and some identify problem ballots for humans to adjudicate. However,

[5] In 2004, in Napa County, CA, a primary election lost 6,000 votes because the scanner was not calibrated to read all types of ink. *See* Kim Zetter, "E-Vote Snafu in California County," Wired, 2004. http://archive.wired.com/politics/security/news/2004/03/62721.

one cannot rely on scanners to do so without error. And scanners cannot detect programming errors or intentional attacks.

23. Logic and Accuracy testing (L&A testing) is intended to test for some of the above problems before the elections, but human error can result in the tests not being correctly completed and equipment malfunction can result in the equipment behaving differently on Election Day. Further, a competent attacker would have the system behave as expected when tested, and maliciously during the election[6].

24. After the votes are read by the optical scanner, they are tabulated electronically by software.

25. In principle, at any point in the above process, software can alter the votes or the tallies. The University of Connecticut Center for Voting Technology Research (VoTeR Center) evaluated the security of AV-OS tabulators, a model also used in Michigan, on the request of the Connecticut Secretary of the State (SOTS) Office, in 2011. They reported[7]: "the memory cards used with AV-OS can be tampered with, thus proving the seriousness of the Hursti Hack. VoTeR Center also discovered new security vulnerabilities of AV-OS. We note that if the memory cards or the AV-OS tabulators are left unattended — within or without the tabulator — they can be tampered with in a matter of minutes. The effects of tampering with the AV-OS and memory cards on the election outcome can be devastating: votes cast on ballots can be reassigned to arbitrary candidates, leading to invalid election results. Subsequent reports by VoTeR Center document additional

[6] Volkswagen's 2L Diesel cars were found to use more emission controls when they were being tested than during normal use. On examination, it was found that their software was written to detect when a test was underway. *See* https://en.wikipedia.org/wiki/Volkswagen_emissions_scandal. In our case, software manipulated without vendor knowledge could also provide testers with the results they expected to see. Then the software could perform differently when used in the election.

[7] VoTeR Center: UConn Center for Voting Technology Research, "Technological Audits of Optical Scan Voting Systems: Summary for 2007 to 2010 Connecticut Elections", Kiayias et al, October 19, 2011, Version 1.1. https://voter.engr.uconn.edu/voter/wp-content/.../VC-TechAudits-2007-2010c.pdf

integrity issues with AV-OS systems. In particular, we determined that even if the memory card is sealed and pre-election testing is performed, one can carry out a devastating array of attacks against an election using only off-the-shelf equipment and without having ever to access the card physically or opening the AV-OS system enclosure. For example, the attacks can lead to the following: Neutralizing candidates: The votes cast for a candidate are not recorded; Swapping candidates: The votes cast for two candidates are swapped; Biased Reporting: The votes are counted correctly by the terminal, but they are reported incorrectly using conditionally-triggered biases." I am not aware if the systems have been modified to resist these specific attacks since they were discovered; regardless, they illustrate the general principle that op-scan systems of this kind are very vulnerable.

26. The method of delivery of the malicious code depends on the type of scanner used. In older op-scan systems, the removable memory used to store counts also stores a computer program to print the results that can be manipulated to print different results.[89] In newer op-scan systems such as the Model 100 also used in Michigan, the removable memory also delivers software updates, and can be used as a means of delivering malicious code[10].

27. Note that one cannot depend on detecting the above types of alteration without a manual review of the paper votes (or, potentially, a forensic audit) because the software process is unobservable and because it is possible for a competent attacker to erase their tracks.

[8] The "Hursti Hack", https://en.wikipedia.org/wiki/Hursti_Hack

[9] *See* Doug Jones,' Comments to Andrew Appel, "Which voting machines can be hacked through the Internet?" Freedom to Tinker (Sept. 20, 2016), https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/

[10] Andrew Appel, Which voting machines can be hacked through the internet?, Freedom to Tinker, (Sept. 20, 2016), https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/

28. In the event that an election outcome were incorrect, the only way to detect this with high certainty is to manually examine the paper votes cast. Rescanning and retabulation of the ballots, even if by another scanner, could lead to the same error or malware, delivered by the same source, having the same influence on the retabulated election outcome. Moreover, where the same scanner is used, as I understand the Michigan recount procedures permit, the problem is exacerbated because any attack on the scanner's software (software that is often referred to as "firmware") would make the recount vulnerable as well. Manual examination of securely stored paper ballots can greatly increase certainty in the outcome.

29. For the above reasons, it is important to make the election audit a standard part of the election process and, where there is no audit procedure, to perform a recount of paper ballots. When paper ballots are available, they provide very reliable independent evidence about voter intent.

30. Given the unhealthy interest demonstrated by foreign powers in influencing the 2016 presidential election, I believe we would send the incorrect signal if we were not to review the voter-verified paper records of the election. We would be making very clear to a potential future attacker how to go about attacking the system. In contrast, if we review the voter-verified paper records from this election, it will serve as an important deterrent to dissuade potential cyberattackers in future elections.

This affidavit was executed on the 30th day of November, 2016 in ________________.

____

POORVI L. VORA

Sworn to before me this 30th day of November, 2016.

____
Notary Public

My Commission Expires: ____________________