AFFIDAVIT OF HARRI HURSTI

1. I declare, under penalty of perjury pursuant to 28 U.S.C. § 1746, that the following is true and correct:

2. I have been a consultant and a co-author of several studies commissioned or funded by various U.S. states and the federal government on computer security. In the area of election security, I am the co-author of several peer-reviewed and state-sponsored studies of election system vulnerabilities. Most notably, I was a co-author of the EVEREST comissioned by the Secretary of State of Ohio (http://hursti.net/docs/everest.pdf), a study of vulnerabilities in Sequoia AVC voting machines (http://hursti.net/docs/princeton-sequoia.pdf), and a study of the Estonian Internet voting system (http://hursti.net/docs/ivoting-ccs14.pdf). In 2005, I developed the Hursti Hack(s), a series of four tests in which I demonstrated how voting results produced by Diebold Election Systems voting machines could be altered. I have served as an expert on electronic voting issues in consultations to officials, legislators, and policy makers in five countries. I received the Electronic Frontier Foundation's EFFI Winston Smith Award in 2008, and the Electronic Frontier Foundation EFF Pioneer Award in 2009 for my research and work on election security, data security and data privacy. I recently founded Nordic Innovation Labs to advise governments around the world on election vulnerabilities. My qualifications and experience are further detailed at the following website: https://nordicinnovationlabs.com/team/harri-hursti/.

How AVC Advantage Machines Work

3. According to VerifiedVoting.org, Montgomery County uses direct recording electronic ("DRE") voting machines called Sequoia AVC Advantage. I have studied these machines in detail, including for a report submitted to the New Jersey Supreme Court.

4. With respect to all DRE machines, including the AVC Advantage, the voter indicates a selection of candidates via a user-interface to a computer; the program in the computer stores data in its memory that (are supposed to) correspond to the indicated votes; and at the close of the polls, the computer outputs (what are supposed to be) the number of votes for each candidate.

5. For the AVC Advantage, electronic ballot definitions are prepared and results are tallied with a Windows application called "WinEDS" that runs on computers at election headquarters in each county. Ballot definitions (contests, candidate names, party affiliations, etc.) are transmitted to the Advantage via a "results cartridge," which is inserted at the election warehouse before the machines are transported to polling places before the election. The votes cast on an individual machine are recorded in the same cartridge, which poll-workers bring to election headquarters after polls close.

6. The AVC Advantage 9.00 includes an "audio kit" containing its own computer board. Any voter who wishes to vote by audio instead of on the large printed buttons-and-lights voter panel is permitted to do so. Voters might wish to vote by audio because of vision impairments, mobility impairments, inability to read, or for any other reason; indeed, voters are not required to state the reason they wish to vote by audio.

7. The audio-kit computer resides on a "daughterboard" inside the cabinet but separate from the main circuit board of the AVC Advantage (which is called the "motherboard").

8. Unlike the motherboard firmware, the firmware of the daughterboard does not reside in read-only memory ("ROM"). It resides in "flash memory"; the flash memory contains the election control program, as well as ballot definitions and other files. Unlike ROM, which cannot be modified without removing and replacing physical computer chips, flash memory can be written and rewritten by the software (or firmware) inside the computer.

AVC Advantage Machines Are Vulnerable and Not Reliable

9. Our study of the AVC Advantage machines found that the AVC Advantage is vulnerable to election fraud, via firmware replacement and other means. Even in the absence of fraud, the AVC Advantage has user interface flaws that could cause votes not to be counted.

10. As we explained in our report, the AVC Advantage is easily "hacked" by tampering with the machine's firmware. Because there is no paper receipt, all electronic records of the votes are under control of the firmware, which can manipulate them all simultaneously.

11. Without even touching a single AVC Advantage, an attacker can install fraudulent firmware into many AVC Advantage machines by viral propagation through audio-ballot cartridges. The virus can steal the votes of blind voters, can cause AVC Advantages in targeted precincts to fail to operate; or can cause WinEDS software to tally votes inaccurately.

12. AVC Advantage Results Cartridges can be easily manipulated to change votes, after the polls are closed but before results from different precincts are cumulated together.

13. The vulnerability of the machines means that good-faith programming errors can also manipulate votes, even without malicious intent. The outdated software renders the machines prone to errors that could affect vote totals.

14. There are also major user interface flaws that may cause inaccuracy in counting votes, including that the AVC Advantage sometimes appears to record a vote when in fact it does not, and vice versa.

These DRE Machines Are Susceptible to Fraud and Tampering

15. The AVC Advantage machines are vulnerable to fraud and inadvertent tampering in a variety of ways. Specifically, the daughterboard and the WinEDS system renders them particularly vulnerable to tampering, fraud, and virus infection.

16. For example, as described above, in addition to the Z80 computer on the AVC Advantage motherboard, the AVC Advantage version 9.00 contains a second computer, called the daughterboard, which is used in audio voting.

17. One can install fraudulent firmware into the daughterboard simply by inserting an audio-ballot cartridge infected with a virus into the slot in the daughterboard. An honest elections official who is unaware of the presence of the virus can do this unwittingly. The process takes one or two minutes. One virus can propagate onto all the WinEDS computers and AVC Advantage voting machines used in a county. This is a very severe vulnerability.

18. Fraudulent firmware in the daughterboard can steal the votes of blind voters, or of any voters who use audio voting, and can selectively cause voting machines to fail on election day in precincts chosen by the attacker.

19. On the version 9 AVC Advantage, the daughterboard does not directly write votes to the Results Cartridge. The motherboard controls the Results Cartridge, and communicates with the daughterboard via messages sent through a cable. When a voter votes using audio, the

daughterboard presents the ballot aurally to the voter, and communicates candidate selections to the motherboard.

20. Audio voters use an input device that is connected to the daughterboard, not the motherboard. Thus it is very easy for fraudulent daughterboard firmware to steal the votes of audio voters, simply by conveying different candidate choices to the motherboard. The votes of disabled voters are even more at risk, on the AVC Advantage, than the votes of those who use the full-face voter panel.

21. In addition, the attacker can cause voting machines to fail in a selected set of precincts. For example, if he disables a dozen or two voting machines in heavily populated districts across the state, then long lines of voters may form, and some voters may leave the polling place before voting. The significance of doing this attack via a daughterboard virus is that a single person can disable voting machines in hundreds of precincts that he chooses, without ever going near any of those machines.

22. To do this, the attacker then programs an audio-ballot virus, replacing the audio-voting software on the daughterboards of all AVC Advantage voting machines in the county.

23. On election day, when each machine is turned on, one of the first things that the motherboard does is to send a message to the daughterboard saying (paraphrase) "load the audio ballot," and the daughterboard normally responds saying (paraphrase) "OK." However, the fraudulent daughterboard software responds with a different message, either one of the following:

- "Cannot load ballot." Then the AVC Advantage (motherboard) will display an error message on the Operator Panel, and the election cannot start.

• A specially crafted message that triggers a buffer overrun bug. This causes the machine to reboot, in an infinite loop, or for as many repetitions as the daughterboard chooses.

24. In either case, the AVC Advantage will fail to start up on the morning of election day, or will be delayed for a chosen number of minutes.

25. The audio-ballot cartridge loaded in the daughterboard contains the name and number of the election district in which the machine will be used. Thus the daughterboard firmware has enough information for an attack on specific precincts. This allows a selective denial of service to specific demographic groups.

26. This general means of manipulating elections is well understood. In Ohio in the 2004 Presidential election, it was widely reported in the press that the misallocation of voting machines led to unprecedented long lines that disenfranchised scores, if not hundreds of thousands, of voters. Selective disabling, instead of misallocation, could produce a similar result.

27. The daughterboard virus is a very elementary attack. Virus programming is not much taught in schools, but unfortunately there are many practitioners of it nonetheless. The number of known computer viruses is enormous. The virus definition file maintained by the virus detection firm Symantec lists over 17 million separate virus "signatures."

28. For this particular virus programming, not even a bachelor's-degree level of skill is necessary. The daughterboard is an Intel-486-compatible computer running a DOS operating system—just like the hardware and software of the IBM PCs from about 1990. Millions of PC users gained familiarity with its scripting tools that would be helpful in creating viruses for the AVC Advantage daughterboard.

29. We found that it is also possible to reverse-engineer the daughterboard firmware. The daughterboard computer is made by Compulab. We were able to find documentation for this computer on the Internet. Compulab sold this computer for many applications, not just voting machines, and development tools are available for it. Using these development tools, an attacker could extract the firmware and reverse-engineer it. Then, using the results of this analysis, he could devise fraudulent firmware of the kind we described above.

30. The motherboard is also vulnerable to malicious daughterboard firmware. One might hope that disabling audio voting would make the motherboard immune to harmful effects from a daughterboard virus. Unfortunately, this is not the case. Because of a mistake Sequoia made in programming the motherboard firmware, the AVC Advantage is vulnerable even if the ballot definition says not to use audio voting.

31. In addition to the daughterboard, the WinEDS system is vulnerable to fraud and tampering. Election workers prepare ballots for the AVC Advantage on WinEDS computers at the election warehouse, or at the board of elections, or other locations. The electronic ballot definition loaded into the Results Cartridge specifies not only the names of the candidates, but several other options about the election. In preparing a ballot definition for the AVC Advantage, one can choose the option to disable audio voting. The (large-format) Results Cartridge with this option setting is then loaded into the (motherboard of the) of the AVC Advantage. This tells the motherboard not to use the daughterboard.

32. The WinEDS election-management software is known to be insecure, based on studies done by the State of California. In our examination we noticed some of the same weaknesses in WinEDS that were previously reported elsewhere.

33. In summary, AVC Advantage voting machines and WinEDS vote-tabulation software are both severely vulnerable to viruses that can alter election results. We have demonstrated the feasibility of creating a computer virus that propagates from AVC Advantage machines to each other, and to WinEDS computers. Such a virus can carry payloads that modify votes inside the AVC Advantage, and modify election and vote databases in WinEDS. The virus can also be programmed to erase itself from voting machines just before the polls close, so as to avoid detection after the fact.

Without A Forensic Evaluation It Is Impossible To Whether the Original Tally Can Be Trusted

34. Because of these numerous vulnerabilities, a full forensic evaluation by independent experts of all of the component's of Montgomery County's Sequoia voting system used in the 2016 presidential general election is the minimum requirement to have any trust at all that the vote was accurately recorded and tallied. This includes:

- Every computer on which Sequoia's WinEDS software was used during the election cycle to prepare Montgomery County's electronic ballot definitions and audio ballots and tabulate results;
- A randomly selected sampling of Sequoia AVC Advantage electronic voting machines, with audio-ballot kits installed and on which ballots were cast. At a minimum, a randomly selected sample of audio-ballot cartridges and results cartridges; and
- The audio ballot cartridge and results cartridge used for those Sequoia Advantage machines.

35. Without such a forensic evaluation, there can be no confidence in the election results.

36. Simply instructing the WinEDS computer to display or print out the results will accomplish nothing. The result will necessarily be identical to the initial computation. This achieves nothing by way of verifying the accuracy or integrity of the results.

37. Similarly, re-uploading the results stored on the results cartridges from the Sequoia AVC Advantage machines used in the election to the WinEDS computer would be an empty exercise. Absent intervening tampering, the results stored electronically on each cartridge will be the same as they were at the time of the initial upload.

38. By contrast, forensic examination by independent experts of the audio-ballot cartridges inside one or more of the AVC Advantage machines used in the election could produce evidence that the software resident on the cartridges had been infected with a virus capable of switching votes from one candidate to another or rendering the affected AVC Advantage machine inoperable on Election Day. It may then be possible to demonstrate the precise nature of any vote-switching routine and its corrupting effect on the recording of votes for a candidate other than the one intended by the voter.

39. Forensic examination of the WinEDS computer used by the county could produce evidence that the WinEDS election management software installed on the computer had been tampered with. Such tampering could be accomplished through direct physical access to the computer, connection of the computer to the Internet at any time before the election, or infection by a virus on one of the audio ballot cartridges that had been connected to the WinEDS computer for programming.

Optical Scan Machines Are Also Vulnerable

40. Optical scan machines can be hacked in a manner that changes election results, and such an attack would likely go undetected during normal pre- and post-election testing. If the scanners are hacked, using them as part of the recount process is likely to result in the same fraudulent election outcome. The only reliable way to detect attacks on the scanners is to recount the paper ballots by hand and compare the results to the electronic tallies.

41. There are a variety of potential attacks that could be levied on optical scan machines.

Attacks on the Precinct Scanners

42. Optical scan voting machines can be manipulated by attackers who are able to modify the election-specific settings on the memory card (sometimes called the "mobile ballot box"). Manipulation of the memory card can either be persistent or "one-time", meaning that if the card is reset but not reprogrammed, the card will be "clean" and the hack will not work until the card is reprogrammed again.

43. Optical scan machines can also be attacked by manipulating the software and operating system in their internal memory (which is sometimes also contained on a memory card, though a separate card from the election data). Manipulation of this kind would afford the attacker total control over the system. To recover from such an attack, the software memory would need to be cleanly reprogrammed, or if the software is stored on a removable memory card, that memory card would have to be physically removed from the scanner and replaced with a known-to-be-secure one. As far as I am aware, Pennsylvania recount procedures do not call for these steps to be performed before scanners are used.

Attacks on Vote Aggregation

44. In some jurisdictions only a single report of votes cast is transmitted and/or published. Common practice to accomplish that is to aggregate votes from other machines used in the precinct to a single machine, and that machine is used to report the results. In this case, if the single aggregation machine is attacked, it can influence votes from all the scanners.

45. With certain voting system vendors it is a recommended practice that all optical scan machines be aggregated into a disabled voter DRE machine before reporting. In this setup, the DRE reserved for a low number of disabled voters actually can influence all the optical scan votes too.

Attacks on Election Media Processors

46. Election media processors are computers which read and/or write many memory cards simultaneously. The EVEREST study cited above found out that a memory card can infect the media processor. An attacker who infects the election media processor in this way can spread the attack to all, or nearly all, scanners that use memory cards written by the processor.

47. Election media processors are typically used by larger jurisdictions and by election services companies that are contracted to program memory cards for many jurisdictions. Attacks on election media processors are therefore likely to affect large numbers of votes.

48. Election media processors have not been certified as of 2008 by the federal Election Assistance Commission or the Federal Election Commission (or, in the case of Ohio by the state), under the legal theory that they are not "vote acting" equipment.

49. These factors make election media processors a particularly dangerous attack vector.

Attacks on High Speed Scanners

50. High-speed scanners are typically used to count ballots from many polling places at a central location. They too face a number of dangerous attack vectors.

51. The controller units of the scanners are typically normal PCs and are subject to a wide array of attacks, including the potential for vote-stealing malware to alter results.

52. The scanner units may be optical mark recognition scanners or digital imaging scanners. Both are hackable. Optical mark recognition scanners can be hacked to misinterpret the ballot and change the recorded vote. A digital imaging scanner can be programmed to manipulate the ballot image. In either case, the recorded vote will not match the voter's intent.

53. There are two major ways high speed scanners are used in an election environment: as scanners producing images into staging areas from which the votes are typically transmitted into a central tabulator over a local area network, or by directing connecting the scanners to a central tabulator.

54. If ballots are transmitted over a local area network, the chain-of-custody of the images is not provable, and images may be manipulated in transmission by network-based attacks.

55. When the scanner is directly connected to the central tabulator, at least one vendor uses special bar codes on the ballots which are commands to the tabulator. Typical commands are "begin batch", "end batch", and "override precinct code". These commands can be transmitted to the machine by ballots that appear under casual human inspection to be normal votes. If an attacker injects them into the set of ballots to be scanned, this can cause real ballots to not be counted, or to be reported in an incorrect jurisdiction.

<u>Attacks on Central Tabulators</u>

56. Central tabulators are normal PCs and and subject to a wide array of attacks, including vote-stealing malware.

57. Tabulator software typically has many features to adjust the vote totals, and these software interfaces can be manipulated by malicious software to alter the reported results.

58. For all these reasons, optical scan votes face a serious threat of being hacked in ways that can alter the outcome of an election. Ballots that are recounted using optical scanners face most of the same threats. The only way to reliably detect such attacks on the election results is to recount the ballots manually, without reliance on potentially hacked election equipment

Executed on the 4TH day of December, 2016 in NEW YORK CITY.

HARRI HURSTI

Subscribed and sworn to
before me this day of

DEC 05 2016

Notary Public

Kershelle Germain
Commissioner of Deeds, City of New York
No. 2-14117
Certificate Filed in New York County
Commission Expires October 1st 2018
The UPS Store | 82 Nassau St. | 212.406.9010

STATE OF NEW YORK
COUNTY OF NEW YORK