Recount Observer Guide and Report Form – Electronic Voting Machines

Before you arrive: Please try to arrive at the recount 15 minutes early. Pack some snacks and a bottle of water, and wear comfortable shoes, as you may be on your feet for long stretches. Bring a notepad and pen; if you are planning to take notes on your phone or to record video, please bring your phone charger.

When you arrive: Introduce yourself to the other observers and the people from the Board of Elections running the recount. Take note of any other campaigns who are represented there, and any media. We would prefer that, instead of commenting on the record yourself, you refer reporters to press@jill2016.com.

If you encounter resistance to your presence: The law states that any watcher present at any recount of ballots or recanvass of voting machines *shall be entitled to examine . . . the voting machine and to raise any objections regarding the same*, which shall be decided by the county board, subject to appeal, in the manner provided by this act." 25 P.S. 2650(c)

Before the recount begins (in a county that uses electronic voting machines): **Demand a forensic audit.** If there is a Stein lawyer present, the lawyer will make this argument. If not, you should press this point BEFORE the recount begins. Ask to speak to the person running the recount.

Here are the points you should emphasize:

1) The Board has the **power** to conduct a meaningful recount. According to the Pennsylvania Supreme Court, "In the computation of the vote, [the Board's] functions are not limited to those of a humanized adding machine." Counting and recounting votes are "acts of discretion." *Appeal of McCracken*, 370 Pa. 362, 365 (1952). Boards of Elections around the state, including in Lehigh County and Philadelphia, have recognized over the past several days that they have discretion in deciding how to conduct a recount. *In other words, they have the authority to decide to grant a full forensic review.*

2) The Board has a **duty** to carefully inspect the voting machines. One of the statutory duties of the Board/Commission is "to inspect systematically and thoroughly the conduct of . . . elections in the several election districts of the county to the end that primaries and elections may be honestly, efficiently, and uniformly conducted." 25 P.S. 2642(g). The Board has also has the power, under the same law, "to *investigate election frauds*, irregularities and violations of this act."

3) Just recanvassing electronic voting machines accomplishes very little. It's like getting a second opinion from the same doctor. Pushing a button to produce an electronic report of results will spit out the same results as the initial tally, drawn from the same software and same memory cards. What we are looking for is confirmation that same software and those memory cards are actually secure and uncompromised.

4) We need an audit to make sure votes were counted properly. Leading experts agree that these voting machines don't provide enough security against cyberattacks. They are susceptible to viruses that can steal votes. A leading expert in this field, J. Alex Halderman, has explained that *every type of machine* used in Pennsylvania "has been examined by security researchers and all have critical security vulnerabilities that could be exploited by attackers to alter the outcome of elections." (See his detailed affidavit included here – which is an expanded and more detailed version of the affidavit that accompanied the petitions, and which describes *each* of the voting machines used in PA.)

5) We are ready for a forensic audit. The Jill Stein Campaign has retained a national team of leading computer experts. They are ready and willing at a moment's notice to conduct a sophisticated analysis of the voting machines to ensure that they have not been compromised. We can provide these experts to the Board, and they can work under the Board's supervision. *The campaign can pay for all of the work.*

6) The Election Code doesn't prevent a forensic audit. Election officials may claim that a section of the Election Code, 25 P.S. § 3154(e), prevents them from doing this. That is wrong. For a recanvass of old-fashioned manual voting machines, the Election Code says that the Board should re-check the machine counters. For electronic voting machines, the Election Code says that the Board should do something "similar." Here, all we are asking is to check that the machines are in good working order—that they are running the software they are supposed to run. That's "similar" to rechecking the counter on an old-fashioned voting machine.

(Also) before the recount begins: **Demand a hand count of paper ballots.** In counties that use paper ballots with optical scanners—electronic machines that read the ballots and tally the votes—the recount must be conducted *differently* than the original count. The best way to accomplish this is to count votes by hand. Even in counties that use electronic voting machines, provisional, military, and other ballots are submitted in paper and should be recounted by hand.

During the recount: Be polite and take lots of notes (including on the form below).

Assuming they refuse to allow a forensic evaluation of the voting machines, there is little substantive information to be gleaned through the "recounts" of the machines. But there are a few things to insist on:

1) Compare the vote totals on the machine print-outs for each precinct with the total number of voters who signed the book, and log any discrepencies. There likely may be one or two discrepencies, but please make note of them, *especially* if there are more votes tallied by the machines than voters who signed the book. Make sure they are reading the machine tallies off of the original print-outs and not new print-outs generated during the recount.

2) Demand a hand recount of all paper ballots.

Absentee, provisional, military, and federal-only ballots are all paper (optical scan) ballots, and each precinct will have a relatively large number of all of these. You should firmly request that these ballots be recounted by hand, and not simply run through the optical scanner. You can cite 25 P.S. § 3154(e)(3), which governs recounts of paper ballots and states that, during a recount/recanvass, the ballots shall be counted using "a different type [of counting mechanism] used for the specific election." Since these paper ballots were originally counted by optical scan, you should insist that they be recounted by hand.

(a) If they refuse to allow a recount by hand: Insist that ONE precinct be re-counted by hand and fed through the scanner, and if the totals match, then they can use that scanner to recount the other precincts. If they want to use more than one scanner, you should insist that all scanners be tested in this way (with a manual count first and then checked against the scanner).

(b) For any ballots counted by hand: You should parnter up with the other Stein observer so that one of you is directly looking at the ballots and the other is making the tally; it is difficult (and slow) to look at the ballot and tally at the same time.

After the recount: Take notes of what happened (using the attached form) and email them to your county captain or to Aquene.

2016 PENNSYLVANIA RECOUNT PRECINCT REPORT

Your Name ________________________________ Your Phone ___________________

Your email address ____

Precinct Location or Number _________________________ **County** _______________

Date(s) of Recount ___________________ Start time __________ End time __________

Voting system used where you observed (circle all that apply):

ES&S iVotronic touchscreen   Diebold / Premier touchscreen   Danaher 1242

Sequoia AVC Advantage   Hart / Intercivic eSlate   Sequoia AVC Edge

ES&S M100 Scanner   ES&S M650 Scanner   Hart / Intercivic eScan

Automark Ballot Marking Device   Other (please specify) __________________________

List the names of the officials conducting the recount and titles (if possible.) Please also note any voting machine company representatives that were present.

____

____

____

List the steps the County Board of Elections will do to conduct this recount:

____

____

____

____

In paper ballot counties, what method will be used to recount the ballots (check one)

__________ Hand count   _________ Scanner

BEFORE THE RECOUNT, Check the following:

Total number of voters listed in the Numbered List of Voters ________________

Total on the Public Counter ________________

Total of Absentees Ballots counted ________________

Total of Provisional Ballots counted ________________

Overall total number of voters (from unofficial or official results) ________________

FOR THE RECOUNT:

Did the county print out or examine the results totals from the county's election results server (computer?)   ________ YES   ________ NO

Did the county print out or examine aggregate results totals from each precinct? (these would be taken from flash cards, disks, cartridges, or "PEBs" and would contain all results from all machines at one precinct.) ________ YES   ________ NO

Did the county print out or examine results totals for individual voting machines?
________ YES   ________ NO

What comparisons of data did the county perform during the recount? (check all that apply)

__________ County main server with individual machine tapes

__________ County main server with precinct result data printout

__________ Individual machine tapes with precinct result data printout

__________ Hand count results (paper ballots) to scanner results

Other (please describe) ____

____

____

Please record the Election Night totals for this precinct (**before the recount**) if available:

	PRESIDENT	US SENATE
Dem	Clinton ________________	McGinty ________________
Rep	Trump ________________	Toomey ________________
Lib	Johnson ______________	Clifford _________________
Grn	Stein ________________	
Con	Castle _______________	

Please record the totals for this precinct **AFTER the recount:**

	PRESIDENT	US SENATE
Dem	Clinton ________________	McGinty ________________
Rep	Trump ________________	Toomey ________________
Lib	Johnson ______________	Clifford _________________
Grn	Stein ________________	
Con	Castle _______________	

RESULTS CHANGED? ________ **YES** ________ **NO**

If yes, please describe the discrepancies ____

____

____

____

____

If there was a discrepancy, did the county compare the number of ballots on the machine tapes with the Numbered List of Voters?

__________ YES __________ NO

If there was a discrepancy, did the county compare the number of ballots on the machine tapes with the pollbooks?

__________ YES __________ NO

Please describe any other efforts to resolve the discrepancy. Please also indicate whether the discrepancy was resolved, and how:

____

____

____

Will the county publish a list of all discrepancies and the resolutions of those discrepancies?

__________ YES __________ NO

Does the county have any plans to print and examine the audit logs from its voting machines?

__________ YES __________ NO

Were any votes, ballots, or totals rejected by the County? __________ YES __________ NO

Reason for rejection: ____

Were any votes or ballots challenged? __________ YES __________ NO

Reason for challenge: ____

If not reported earlier, please describe County's plans / process for reporting results of recount, and describe process for deciding challenges:

____

____

____

IMPORTANT: Please write up a diary or narrative of your experience on another sheet of paper and attach. Also, it would be wonderful if you could have someone record a video of your recollections and thoughts about this experience immediately after leaving the recount (perhaps you could film this in front of the courthouse?)

AFFIDAVIT OF J. ALEX HALDERMAN

J. ALEX HALDERMAN, being duly sworn, deposes and says the following under penalty of perjury:

1. My name is J. Alex Halderman. I am a Professor of Computer Science and Engineering and the Director of the Center for Computer Security and Society at the University of Michigan in Ann Arbor, Michigan. I submit this Affidavit in support of the petitioners.

2. I have a Ph.D., a Master's Degree, and a Bachelor's Degree in Computer Science, all from Princeton University.

3. My research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Among my areas of research are software security, data privacy, and electronic voting.

4. I have authored more than seventy articles and books. My work has been cited in more than 4,700 scholarly publications. I have served on the program committees for thirty research conferences and workshops, and I co-chaired the USENIX Election Technology Workshop, which focuses on electronic voting security. I received the John Gideon Award for Election Integrity from the Election Verification Network, the Alfred P. Sloan Foundation Research Fellowship, the IRTF Applied Networking Research Prize, and the University of Michigan College of Engineering 1938 E Award for teaching and scholarship.

5. I have published peer-reviewed research analyzing the security of electronic voting systems used in Pennsylvania, other U.S. states, and other countries. I was part of a team of experts commissioned by the California Secretary of State to conduct a "Top-to-Bottom" review of the state's electronic voting systems. I have also investigated methods for improving the

security of electronic voting, such as efficient techniques for testing whether electronic vote totals match paper vote records.

6. My full curriculum vitae, including a list of honors and awards, research projects, and publications, is attached as Exhibit A.

Context: Cyberattacks and the 2016 Presidential Election

7. The 2016 presidential election was subject to unprecedented cyberattacks apparently intended to interfere with the election. This summer, attackers broke into the email system of the Democratic National Committee and, separately, into the email account of John Podesta, the chairman of Secretary Clinton's campaign. Exhibits B and C. The attackers leaked private messages from both hacks. Attackers also infiltrated the voter registration systems of two states, Illinois and Arizona, and stole voter data. Exhibit D. The Department of Homeland Security has stated that senior officials in the Russian government commissioned these attacks. Exhibit E. Attackers attempted to breach election offices in more than 20 other states. Exhibit F.

8. Russia has sophisticated cyber-offensive capabilities, and it has shown a willingness to use them to hack elections elsewhere. For instance, according to published reports, during the 2014 presidential election in Ukraine, attackers linked to Russia sabotaged Ukraine's vote-counting infrastructure, and Ukrainian officials succeeded only at the last minute in defusing vote-stealing malware that could have caused the wrong winner to be announced. Exhibit G. Countries other than Russia also have similarly sophisticated cyberwarfare capabilities.

9. If a foreign government were to attempt to hack American voting machines to influence the outcome of a presidential election, one might expect the attackers to proceed as follows. First, the attackers might probe election offices (or the offices of election service vendors) well in advance to find ways to break into the computers. Next, closer to the election,

when it was clear from polling data which states would have close electoral margins, the attackers might spread malware into voting machines in some of these states, manipulating the machines to shift a few percent of the vote to favor their desired candidate. One would expect a skilled attacker's work to leave no visible signs, other than a surprising electoral outcome in which results in several close states differed from pre-election polling.

The Vulnerability of American Voting Machines to Cyberattack

10. As I and other experts have repeatedly documented in peer-reviewed and state-sponsored research studies, American voting machines have serious cybersecurity problems. Voting machines are computers with reprogrammable software. An attacker who can modify that software by infecting the machines with malware can cause the machines to provide any result of the attacker's choosing. As I have demonstrated in laboratory tests, in just a few seconds, anyone can install vote-stealing malware on a voting machine that silently alters the electronic records of every vote.[1]

11. Whether voting machines are connected to the Internet is irrelevant. Sophisticated attackers such as nation-states have a developed a variety of techniques for attacking non-Internet-connected systems.[2] Shortly before each election, poll workers copy the ballot design from a regular desktop computer in a government office (or at a company that services the voting machines) and use removable media (akin to the memory card in a digital camera) to load the ballot design onto each machine. That initial computer is almost certainly not well enough secured to guard against attacks by foreign governments. If technically sophisticated attackers infect that computer, they can spread vote-stealing malware to every voting machine in the area.

[1] A video documenting this result is publicly available at https://youtu.be/aZws98jw67g.

[2] A well known example of this ability, which is known as "jumping an airgap", is the Stuxnet computer virus, which was created to sabotage Iran's nuclear centrifuge program by attacking factory equipment that was not directly connected to the Internet: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Most voting machines also have reprogrammable software ("firmware") that can in many cases be manipulated well in advance of the election to introduce vote-stealing malware. Technically sophisticated attackers can accomplish this with ease.

12. While the vulnerabilities of American voting machines have been known for some time, states' responses to these vulnerabilities have been patchy and inconsistent at best. Many states, including Pennsylvania, continue to use out-of-date machines that are known to be insecure.

13. Procedural safeguards used by Pennsylvania and other states to protect their voting equipment are inadequate to guard against manipulation of the election outcome via cyberattack. These inadequate safeguards include tamper evident seals, protective counters, and test decks.

14. Tamper evident seals do not protect against remote electronic attackers, and may not even defend against local attackers. The types of seals typically used for voting equipment can be bypassed without detection using readily available tools.[3] For some seals, these include screwdrivers and hair dryers. By bypassing the seals, an attacker with physical access to the voting machines can modify their internal programming to make them output fraudulent results.

15. Malware installed on a voting machine can subvert the protective counter by changing its value in the machine's computer memory. Malware can subvert test decks by refraining from cheating when only a small number of ballots have been scanned (as is the case when a test deck is used), or by only cheating at a specified time of day (electronic voting machines typically have internal clocks).

[3] https://www.cs.princeton.edu/~appel/voting/SealsOnVotingMachines.pdf

Pennsylvania's Voting Machines Are Among The Most Vulnerable In The U.S.

16. Paper ballots are the best and most secure technology available for casting votes. Optical scan voting allows the voter to fill out a paper ballot that is scanned and counted by a computer. Electronic voting machines with voter-verified paper audit trails allow the voter to review a printed record of the vote he has just cast on a computer. Only a paper record documents the vote in a manner that cannot later be modified by malware or other forms of cyberattacks.

17. More than 70% of American voters have their votes recorded on some form of paper, which provides permanent evidence of their intent in the event of a post-election recount. In Pennsylvania, less than approximately 20% of votes are cast using paper ballots or voter-verified paper audit trails. The remaining approximately 80% are cast on paperless direct-recording electronic (DRE) computer voting machines that do not create a paper record of each vote.

18. Paperless DRE voting machines have been repeatedly shown to be vulnerable to cyberattacks that can change or erase votes, cast extra votes, or even infect the software used to tabulate results. Since paperless DREs do not generate a physical record of the vote, these attacks may be difficult or impossible to detect or to reverse. There is a broad scientific consensus that paperless DREs do not provide adequate security against cyberattacks.

19. To my knowledge, there are six models of DREs presently in use in Pennsylvania. Every one of these models has been examined by security researchers (in some cases, repeatedly), and all have critical security vulnerabilities that could be exploited by attackers to alter the outcome of elections. These vulnerabilities include architectural weaknesses that cannot be repaired through software updates. As a result, every DRE in use in Pennsylvania is vulnerable to cyberattacks.

20. The vulnerable DREs used in Pennsylvania include:

21. **Hart InterCivic eSlate** — This model of machine was examined by security experts as part of the California "Top to Bottom" election technology review[4] and the Ohio EVEREST election system security review[5]. Both studies found significant vulnerabilities, and California subsequently decertified the machine.[6] The memory cards used by eSlates to transfer votes to a central counting computer are vulnerable to undetectable tampering. The internal security mechanisms of the machines are easily defeated, enabling malicious software to change or erase votes, cast extra votes, or modify the eSlate's software or the software of the JBC, the machine used to tabulate votes. These vulnerabilities could allow attackers to compromise large numbers of machines and alter the election outcome.

22. **Sequoia (Dominion) AVC Advantage** — This model of machine has been studied by multiple groups of security researchers. I have extensively analyzed the AVC Advantage, and I published a peer-reviewed security study of the machines in 2009. My study demonstrates that malware can infect the machines and alter votes. Such malware can spread to the machines via the removable memory cartridges that are used to program the ballot design and offload votes.[7] My research additionally shows that such malware can defeat all of the hardware and software security features that are used by the machines. A separate group of researchers performed a security review that also concluded the AVC Advantage has significant vulnerabilities, including that it would be

[4] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/hart-amended-recert-final-120707.pdf

[5] http://www.patrickmcdaniel.org/pubs/everest.pdf

[6] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/hart-amended-recert-final-120707.pdf

[7] https://jhalderm.com/pub/papers/avc-evt09.pdf

straightforward to install vote-stealing malware by replacing one firmware chip.[8] Deficiencies of this voting machine are not limited to security vulnerabilities: in the 2008 New Jersey Republican primary, 37 of these machines exhibited a software bug in which the number of votes recorded was higher than the number of voters.[9]

23. **Danaher Shouptronic 1242** — This model of machine was introduced in 1984 and has not had its security features updated in more than 30 years. Cyberattacks have become significantly more sophisticated during that time, and the security features in the machine are unlikely to be able to defend against today's attackers. Researchers at Lehigh University have analyzed the Shouptronic's computer architecture and shown that it is constructed in a very similar manner to the AVC Advantage.[10] This computer architecture subjects the machines to many of the same attacks. Attackers can replace the machines' ROM chips to cause the machines to output fraudulent results. The machines' design makes it extremely likely that malware can infect the machines via the removable memory cartridges that are used to program the ballot design and retrieve vote totals. The Shouptronic has also already been problematic in past elections,[11] malfunctioning and causing significant delays in voting multiple times in Pennsylvania, Tennessee, and Ohio.

24. **Premier/Diebold (Dominion) AccuVote TSX** — I performed a security analysis of the AccuVote TSX as part of the California Top-to-Bottom review[12], and the machine was also studied as part of Ohio's Project EVEREST[13] and by independent security

[8] https://mbernhard.com/advantage-insecurities-redacted.pdf
[9] https://www.usenix.org/legacy/event/evtwote09/tech/full_papers/appel.pdf
[10] https://verifiedvoting.org/downloads/2008Danaher1242-full.pdf
[11] https://w2.eff.org/Activism/E-voting/infosheets2006/ELECTronic1242.pdf
[12] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-102507.pdf
[13] http://www.patrickmcdaniel.org/pubs/everest.pdf

researchers[14]. All of these studies found extremely serious security problems. This machine, along with its predecessor the AccuVote-TS, which I studied extensively in a 2007 security review[15], can be exploited by attackers to alter election results. The security features built into the machines are inadequate to defend against cyberattacks, and vote-stealing malware can spread on the machines' removable memory cards. If attackers infect counties' election management system computers, the attacker can spread vote-stealing malware to every voting machine in the county. Moreover, these machines rely on Windows CE as their operating system, software that has not been supported by Microsoft in several years,[16] and has been shown to have significant vulnerabilities itself, beyond those of the election-specific software.[17] A local attacker with physical access to the machines can additionally tamper with them by manipulating the machines' removable memory cards. Access to these cards is protected using a low security lock that can be picked using only a BIC pen.[18] California decertified the Accuvote TSX in 2007.[19]

25. **Sequoia (Dominion) AVC Edge** — Also decertified by California in 2007,[20] this machine has vulnerabilities similar to those of the TSX and the eSlate. In the California Top-to-Bottom review, security experts found that remote attacks could spread malware to the machines and change, steal, or add votes. Furthermore, such malware can persist even if election workers reinstall an uncorrupted version of the election software. The

[14] http://www.blackboxvoting.org/BBVtsxstudy.pdf

[15] http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/ts06EVT.pdf

[16] https://support.microsoft.com/en-us/lifecycle/search?alpha=Microsoft%20Windows%20CE%20.NET%204.0

[17] https://www.cvedetails.com/product/1079/Microsoft-Windows-Ce.html?vendor_id=26

[18] Shown in this video demonstration: https://www.youtube.com/watch?v=vqNJL0fYwSk

[19] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-102507.pdf

[20] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/sequoia-100109.pdf

California study further discovered that malicious software on the machines could conceal vote-tampering from pre-election testing, hiding manipulation of votes and making the machine output appear otherwise normal. The election software running inside the AVC Edge can also be tampered with by a local attacker with physical access to the machine by replacing a memory card inside the machine's case. I demonstrated this vulnerability by hacking one AVC Edge to make it run the arcade game Pac-Man.[21] A real attacker could just as easily modify the software to make the machine cheat in elections.

26. **Election Systems & Software iVotronic** — The iVotronic was studied by security experts as part of Project EVEREST.[22] The investigation found that firmware on these machines contained buffer overflow vulnerabilities, which could be exploited to infect the machines with malware and alter the election outcome. Further vulnerabilities in the machines include that the Personalized Electronic Ballot module (PEB), which is used to program the ballot design before the election, had only trivially circumventable security protections. The EVEREST researchers also found that the cryptographic keys used by the machines to encrypt votes could be easily extracted by attackers, who could then read or manipulate the vote data.

Examining the Physical Evidence is the Only Way to Ensure the Integrity of the Election

27. One explanation for the results of the 2016 presidential election is that cyberattacks influenced the result. This explanation is plausible, in light of other known cyberattacks intended to affect the outcome of the election; the profound vulnerability of American voting

[21] https://jhalderm.com/pacman/

[22] http://www.patrickmcdaniel.org/pubs/everest.pdf

machines to cyberattack; and the fact that a skilled attacker would leave no outwardly visible evidence of an attack other than an unexpected result.

28. The only way to determine whether a cyberattack affected the outcome of the 2016 presidential election is to examine the available physical evidence—that is, the paper ballots (where available), paper audit trail records (where available), and the voting equipment itself.

For DREs With Paper Trails, The Paper Trail Must Be Recounted By Hand

29. For DRE voting machines that generate paper vote records (VVPAT records), the paper must be examined in order to detect potential cyberattacks. Simply commanding the machines to output the vote totals again would not reliably uncover an attack. This is because any attack on the machines during the election would likely have changed the digital record of the votes stored in the voting machines' memory (as well as in any external memory cartridges or cards). Therefore, the digital records do not reliably preserve voters' intent. In contrast, a manual examination of the VVPAT record would expose this style of cyberattack.

For DREs Without Paper Trails, A Forensic Examination Must Be Conducted

30. Most of Pennsylvania's votes are recorded on DRE voting machines that do not generate any paper record of the individual votes. The only way to reliably determine whether the election outcome on these machines was changed by a cyberattack is to forensically examine the election equipment. A complete forensic examination would include examining the machines' hardware and software, their removable media, and the election management system computers used to program the machines and aggregate election results.

31. Forensic examination could reveal evidence of an attack, such as successful attempts to spread malware to the machines. Such evidence could include malware itself, signs of remote intrusion in the election management system, or indicators that digital vote records or other files

were manipulated or deleted. If a forensic examination can determine the manner in which the machines were compromised, it might also allow manipulation of the election result to be corrected.

For Optical Scan Paper Ballots, The Ballots Must Be Recounted By Hand

32. For ballots cast through optical scanners, a manual recount of the paper ballots, without relying on the electronic equipment, is necessary to reliably detect possible hacking. Using optical scan machines to conduct the recount, even after first evaluating the machines through a test deck, is insufficient to detect potential cyberattacks. Attackers intending to commit a successful cyberattack could, and likely would, create a method to undermine any pre-tests.[23]

33. If the optical scanners were attacked by infecting them with malware, such malware might still be active in the scanners during the recount. Recounting the ballots using an infected scanner would likely yield the same results as the original count, despite the results being wrong. If attackers managed to compromise the count during election day but in a manner that did not persist on the machines, machine recounts would still be insufficient. Attackers who were able to infect the machines before the election likely would be able to attack them again, perhaps using the same methods, prior to the recount. The dates and the procedures of the recount are widely publicized, so attackers would know when to strike. This would result in the scanners producing the same incorrect results when the ballots were scanned again.

34. In contrast to machine recounts, a manual recount, where the paper ballots are inspected by humans, can reliably detect any cyberattack that might have altered the election

[23] Volkswagen used a similar strategy to conceal the way it circumvented EPA emissions tests: http://www.reuters.com/article/us-volkswagen-emissions-audi-idUSKBN1370Q3

outcome on the optical scanners. A manual recount is the best way, and indeed the only way, to ensure public confidence that the results are accurate, authentic, and untainted by interference.

35. Manual recounts are not necessarily more time-consuming than recounting using optical scanners, particularly when only one race is being counted. A manual recount focuses on a single contest, and human observers typically proceed by sorting the ballots into stacks according to the chosen candidate and then counting the ballots in each stack. This is an efficient and straightforward process. If scanners are used, the scanners must be programmed and tested, new removable media must be located and programmed, and the ballots must be fed into the scanner by humans. These steps are not necessary when hand counting is used.

36. The paper ballots used in Pennsylvania can be counted much more easily and reliably than the punched card paper ballots that were recounted in Florida during the 2000 presidential election. Punched card ballots are fragile, so each time they are counted, the record of voters' intent may be inadvertently altered. They are also difficult to interpret, sometimes requiring a magnifying glass to discern whether the voter intended to make a mark. Pennsylvania's optically scanned paper ballots are a completely different technology. They create a persistent and readily interpretable record of voters' intent that does not suffer from these problems, and they can be counted efficiently and accurately in a manual recount.

37. Examining the available physical evidence, including paper ballots, paper vote records, and the voting equipment itself, will set a precedent that will provide an important deterrent against cyberattacks on future elections. By performing a rigorous recount now in a method that would detect cyberattacks affecting the outcome (that is, by thoroughly examining this physical evidence), we send a strong signal to attackers that any future computer-based tampering efforts are likely to be caught.

This affidavit was executed on the 30th day of November, 2016 in Ann Arbor, Michigan.

J. ALEX HALDERMAN

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

Tobin C Darnell

Notary Public

My Commission Expires: 04-04-2018

TOBIN C. DARNELL
NOTARY PUBLIC, STATE OF MI
COUNTY OF WASHTENAW
MY COMMISSION EXPIRES Apr 4, 2018