Exhibit 11

AFFIDAVIT OF HARRI HURSTI

I declare under penalty of perjury and under the laws of Michigan that the following is true and correct, and that I am physically located outside the geographic boundaries of the United States, Puerto Rico, the United States Virgin Islands, and any territory or insular possession subject to the jurisdiction of the United States.

1. In 2005, I developed the Hursti Hack(s), a series of four tests in which I demonstrated how voting results produced by the Diebold Election Systems voting machines could be altered. I submit this Affidavit in support of a hand recount of all ballots in Michigan.

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). I have served as an expert on electronic voting issues in consultations to officials, legislators, and policy makers in five countries. I received the EFFI Winston Smith Award 2008, and the EFF Pioneer Award 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/.

Opinion

3. Many of the models of voting machines and other election infrastructure used in Michigan were previously analyzed by state-sponsored security reviews, including the EVEREST report (http://hursti.net/docs/everest.pdf) commissioned by the Secretary of State Ohio, and were shown to be vulnerable to demonstrated attacks. Due to the shortness of time, I have not been able verify which of these attacks are feasible on the systems used in one or many of the Michigan jurisdictions. It is possible that critical parts of the election infrastructure are processed with equipment which has never been submitted for certification.

4. 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.

5. The following attack vectors expose optical scan election results to potential hacking

Attacks on Precinct Scanners

6. 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.

7. 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. Michigan recount procedures do not require these steps to be performed before scanners are used.

Attack on Vote Aggregation

8. 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.

9. 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

10. 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.

11. 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.

12. 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.

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

Attacks on High speed Scanners

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

Attacks on Central Tabulators

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

21. 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.

22. 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 2nd day of December, 2016 in Helsinki, Finland.

HARRI HURSTI