# AFFIDAVIT OF DUNCAN A. BUELL

DUNCAN A. BUELL, being duly sworn, deposes and says the following under penalty of perjury.

1. I am a professor of Computer Science and Engineering at the University of South Carolina. I submit this affidavit in support of petitions to recount/recanvass the vote in Allegheny County.

2. In my opinion, the electronic voting system used by Allegheny County, called the iVotronics system, is vulnerable to malicious interference and inadvertent error. The system is unreliable. The only way to be sure of an accurate tally of the vote in this election is to conduct a forensic analysis of the machines and software. Such an evaluation could be accomplished expeditiously, in a few short hours, and would allow us to know whether the vote tally in Allegheny County was accurate.

## Qualifications and Relevant Employment History

3. In 1971, I earned a B.S. in Mathematics from the University of Arizona. The following year, I earned an M.A. in Mathematics from the University of Michigan. In 1976, I earned a doctorate in Mathematics, with an emphasis in number theory, from the University of Illinois at Chicago. A copy of my resume is available on my university website at http://www.cse.sc.edu/duncanbuell.

4. Since 2000, I have been a Professor in the Department of Computer Science and Engineering at the University of South Carolina. From 2000 to 2009, I served as Chair of that department. During 2005-2006, I served as Interim Dean of the College of Engineering and Information Technology at the University of South Carolina.

In my management capacity as department chair, my duties also included the management of the college's information technology staff and its network and computer center, which included 9 instructional labs with approximately 250 desktop computers. I was also responsible for the management and operation of cluster computers, file and mail servers, and the college's network infrastructure.

5. Prior to 2000, I was for just under 15 years employed (with various job titles and duties) at the Supercomputing Research Center (later named the Center for Computing Sciences) of the Institute for Defense Analyses, a Federally Funded Research and Development Center (FFRDC) supporting the National Security Agency. Our mission at SRC/CCS was primarily to conduct research on high performance computing systems and computational mathematics to ensure that those computing systems would be suitable for use by NSA, since the NSA workload has technical characteristics different from most high-end computations like weather modeling. While at IDA I played a leading role in a group that received a Meritorious Unit Citation from Director of Central Intelligence George Tenet for what was then "the largest single computation ever made" in the U.S. intelligence community.

6. In 2013, I was elected a Fellow of the American Association for the Advancement of Science. In 2016, I was appointed to the NCR Chair in Computer Science and Engineering at the University of South Carolina.

7. My current research interests include electronic voting systems, digital humanities, high performance computing applications, parallel algorithms and architecture, computer security, computational number theory, and information retrieval.

Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured on each of these topics.

8. Since about 2004 I have been working with the League of Women Voters of South Carolina (LWVSC) as an unpaid consultant on the issue of electronic voting machines. South Carolina uses statewide the ES&S iVotronic terminals and the corresponding Unity[1] software. Beginning in summer 2010, I worked with citizen volunteer activists Frank Heindel, Chip Moore, Eleanor Hare, and Barbara Zia on acquisition by FOIA of the election data from the November 2010 general elections in South Carolina and on the analysis of that data. That work, based on data we acquired by FOIA, culminated in an academic paper that was presented at the annual USENIX EVT/WOTE (Electronic Voting Technology Workshop/Workshop on Trustworthy Elections) conference in August 2011. My work with the LWVSC has continued, in that when the state of South Carolina acquired the 2010 election data from the counties and posted it on the SCSEC website, I analyzed that data as well.

**Basis for My Opinions**

9. I base the opinions in this affidavit on my knowledge, skill, training, education, and experience: I have been programming computers for more than 45 years and have been employed as a computer scientist for more than 35 years, working with

[1] Unity is the election management software suite, a number of programs that run on a Microsoft computer at county headquarters and perform such tasks as initializing the database with jurisdiction and candidate information, configuring the ballot styles, collecting the vote totals from the PEBs into the master database of votes and log information, and producing reports of votes by candidate and precinct as well as the log files and cast vote record files referred to below.

computers and computer applications and operations and management of large computer networks, including file and mail servers that utilize the Internet.

10. I have also used for my opinions the analysis of the ES&S iVotronic system and the Unity software done for Ohio Secretary of State Jennifer Brunner and published 7 December 2007. This is the "EVEREST Report" and is still the best and most complete analysis of the iVotronics and their accompanying software and procedures. I am also familiar with the report produced for the state of Florida ("the Yasinsac report") after the 2006 election in Sarasota, Florida resulted in a very high undervote in the race for U. S. Representative.

11. I also base my opinions on my analysis of ES&S election data using computer programs I have written. I first wrote these programs to analyze the 2010 General Election data from South Carolina. I have subsequently analyzed the 2012, 2014, and 2016 data from South Carolina. I have also used my programs to analyze data from from Hidalgo County, Texas and from Venango County, Pennsylvania, at the request of election officials there. I believe I have more experience in doing this analysis of ES&S iVotronic data than anyone else, possibly including employees of ES&S itself.

**The ES&S iVotronics Machines and Accompanying System Are Riddled with Software and Procedural Vulnerabilities**

12. The iVotronics machines and software systems[2] are not secure or reliable. They are susceptible to both intentional and malicious interference as well as errors

[2] I will refer throughout this affidavit to "the iVotronics" and mean by that the entire system of which the iVotronic is the voting machine itself. The system includes also the handheld PEB devices, the flash memory cards inserted into and removed from the iVotronic, and the Unity software and stored data used (usually) at county headquarters.

resulting from inadvertent or sloppy mistakes. The only way to be sure of the accuracy of the vote is to carefully examine the machines and the systems they ran.

***The Machines Are Vulnerable to Intentional Interference***

13. The EVEREST report documented a number of software flaws, many of which relate to the reliability or security of the system. The Yasinsac report describes a naïve, indeed juvenile, password structure that could easily be circumvented by any insider and that could be circumvented without enormous difficulty by an outside attacker.

14. The EVEREST report also refers to numerous buffer overflow vulnerabilities that would permit the installation of malicious software. And, when done by a skilled attacker, the malicious code could eventually erase itself to leave no trace.

15. In addition, an attacker could use a PEB[3] or a PEB emulator (a Palm Pilot with the same infrared protocol was used in the test) to masquerade as a valid PEB, open an iVotronic as if for voting, and upload malicious code.

16. Election officials and vendors often justify the security of their systems by pointing to the proprietary nature of the hardware and software, suggesting that no one who was not permitted to use a voting system could get access to one. This argument is incorrect; I purchased two iVotronics with PEBs myself on eBay. It would be relatively straightforward to create a rogue PEB through which to spread malware (thus not needing

[3] Personal Electronic Ballot: This is a handheld device slightly smaller than a paperback novel. Proper procedure is that the precinct poll manager will use one particular PEB to open and close the iVotronics at the beginning and ending of Election Day, and that regular poll workers will use a different set of PEBs to open the iVotronic for each voter and to load onto the machine the particular ballot style for that voter's jurisdictions.

the Palm Pilot or similar device). In my experience as a poll observer in South Carolina in the 2016 General Election, I noticed that it would have been easy for a voter to shield from view the PEB slot while voting and thus insert a rogue PEB to upload malicious code.

***The Machines Are Vulnerable Even If They Are Not Connected to the Internet***

17. It is a frequent claim by election officials that the voting machines cannot be corrupted because they are never "connected" to the Internet. This is a statement that is only true if literally none of the computing hardware—or any removable media connected to the computer—has ever been connected to any computer that has been connected to the Internet.

18. To provide background for what is really meant by "not connected," one must remember what apparently took place with the Stuxnet virus. Stuxnet was apparently a joint US and Israeli effort to sabotage the Iranian efforts to produce nuclear weapons. Part of the Iranian nuclear program involved specific centrifuges for concentrating uranium. None of those centrifuges were ever "connected" to the Internet, and yet Stuxnet was inserted into the Iranian nuclear network and caused a large number of centrifuges to self-destruct. Part of the distribution of the Stuxnet virus apparently involved hiding it on flash memory drives that were sprinkled in parking lots. When curious people picked them up and inserted them into computers inside the nuclear program network, Stuxnet was inserted into the system.

19. Indeed, this vulnerability is well known. My colleagues and I received a briefing from the FBI a few years ago warning faculty travelling to conferences not to

allow a "friend" to offer us a flash drive to share documents, because the "friend" could easily install a virus in this way.

20. In short, any sort of electronic connection can lead to the insertion of malware into the computer thus connected.

21. In most electronic voting systems in the United States, including the iVotronics, a county election official uses the computer running Unity to prepare the ballot styles for each of the precincts and jurisdictions. The county computer then prepares the PEBs for use on Election Day by loading the PEBs with the ballot styles for the individual precincts. The county computer would normally also erase the files on the memory cards to be inserted into the iVotronics. That represents the outward path from county headquarters to the individual iVotronics.

22. On the inbound path, at the end of Election Day, the memory cards and the PEBs come back from the individual precincts and are connected to the county computer. Presumably this is the same computer from which results are provided to the media and the public at the end of Election Day.

23. It can only be argued that this voting system as a system is "not connected" to the Internet if it is the case that none of the computing equipment has been connected at any time. This means that the Unity computer will never have had its operating system or its code updated since the system was first brought up (unless, of course, the updates were to come on some medium like a CD from a trusted source like the ES&S vendor). This means that flash drives that carry results from the Unity system to a computer on the network that sends the results to the news media (or any flash drive that has ever been

inserted into a computer on a network) must never be reused and inserted back into the Unity system.

24. It is possible that all these security measures are in place in every single county in the state. In my experience, however, this is extremely unlikely, and thus a forensic analysis would need to look at and verify that all these protocols were followed.

***The Machines Are Also Vulnerable to Inadvertent Errors that Render Them Unreliable***

25. The complexity of the iVotronics system itself leaves it vulnerable to error. For example, the iVotronics are supposed to be opened and closed with a single PEB in each precinct, with that PEB used only for opening and closing. Since at closing the vote totals are collected into the PEB, and the totals from the closing PEB are used for totaling into the Unity database at county headquarters, it can (and does) happen that poll managers don't follow directions and use multiple PEBs for opening and closing, and that not all the vote totals are accumulated into the county database. PEBs can also fail in a precinct.

26. I have also seen examples when iVotronics would not open normally at the beginning of Election Day, were opened later by a technician, but then at the end of Election Day the paper tape produced by the precinct poll manager said "Machine not opened". This has led to the votes in those machines not being accumulated into the official count at the county level and thus effectively not being counted.

27. Another failure in the software comes when the ballot definition in the iVotronic is different from that at county headquarters. If the county system lists two

races for county council, say, and the ballot definition in the iVotronic only has one race, then what happens is essentially that vote totals from that point on down to the bottom of the ballot are shifted up one row and added into the wrong row's totals.

28. Similar failures can occur when memory cards fail, or when iVotronics will not allow themselves to be closed for some reason.

***Only a Forensic Evaluation Can Determine Whether Votes Were Properly Counted***

29. Only a forensic evaluation, including an examination of the election management system and software, will reveal whether the official tally of votes is reliable or whether the voting process was disrupted by malicious attack or other error.

30. With respect to malicious interference, a forensic evaluation would allow investigators certainly to determine if a systematic failure of proper procedures had occurred. I would expect random failures to occur, reflecting the chaos of Election Day and the imperfections of poll workers. Systematic issues, however, would show up as anomalies that might well be intentional. The ability to drill down to precinct level data allows one to compare anomalies and "errors" against voting preferences and demographics, and a forensic analysis with statistics would spot such anomalies.

31. Such an investigation could be accomplished expeditiously. For the purpose of my data analysis, I would need the EL152 event log file, the EL155 cast vote record, the EL68A system file, and the EL30A results file. I have never been told in South Carolina, Hidalgo County (TX), or Venango County (PA)—each places I have worked and performed analyses of election data—that obtaining this data was difficult; it can be produced using the Unity software from the county database. Analysis of this data using

my programs for the entire 2016 South Carolina data (2.1 million total votes) took about *three hours*' compute time. Depending on the number of exceptional cases to be looked into, an in-depth examination of these cases should take only a small number of days, much less time if the exceptions are usually benign. (For example, I produce a list of iVotronics that appear in the event log but have no cast vote record. It has happened that such a machine has not had its votes counted, which is a serious error, but what I usually see here is that such a machine never did get properly opened and was never used; that fact can be determined by a very quick scan of the event log that takes only seconds.)

32. I have conducted forensic analyses of these machines to ensure that the voting tallies were accurate. Beginning with the 2010 General Election in South Carolina, I obtained the voting data and wrote my own programs to verify that all the votes had in fact been counted and that the election data was at least internally consistent. I have rewritten my programs several times, most recently following the 2016 General Election. I have used four data sources in my analysis, which are data files published as public records by the South Carolina State Election Commission on their website http://scvotes.org.

33. First, I examine the event log file from each iVotronic. It lists the events recorded in each machine since the most recent time the internal file was erased. From this file I get the serial number of the iVotronic machine, the serial numbers of the PEBs used for most of the events, the timestamp when the events occurred, and the code number and expanded English text of the event itself. For example, code 1510 is "Vote cast by voter." From this file I can determine that the internal memory was zeroed before

use for this election, how many votes were cast on each iVotronic, which PEB was used for opening and for closing, verify that the iVotronic was closed and its internal data written to the memory card, and so forth. This allows me to determine the number of votes cast on each machine, the fact that the machines were cleared of votes and that the data was written to the memory cards, and whether or not the machine was functioning properly on Election Day. By knowing which PEB was used for closing I also know which PEB serial numbers to look for in the system log to verify that the vote totals were correctly uploaded to the county database. I have repeatedly observed instances of "cranky" iVotronics that could not be closed or that had bad memory cards, or were not functioning properly; knowing that such machines exist (by serial number) allows me to verify elsewhere that other methods have been used to account properly for the votes in those iVotronics.

34. Second, I examine the system log for the Unity software running on a Microsoft computer at county headquarters. From this file I can determine that the county database was cleared before Election Day, that the correct number of votes were uploaded from the PEBs (by serial number) for a given precinct, that the memory card data was uploaded to the county database, and so forth. It is in this file that one can find the log of ballot definition differences between the county version and the version in each iVotronic. This allows me to determine that the data (including vote counts) from machines known to have been used for voting has been uploaded correctly.

35. Next, I look at the data of the actual cast vote record, in a randomized order, and with no identifying information about which voter cast which ballot. From this

file I can produce vote counts for each iVotronic, each ballot style, each precinct, and each race.

36. Finally, I examine one of several "results" files that are produced by the Unity software. From this I can determine for each precinct and each race the number of iVotronic votes recorded from the PEBs, the number of votes that might have been recorded by reading directly from the memory cards, and the number of paper or absentee ballots. (If the county chooses not to print this information, it might not appear.)

37. My programs count votes at the precinct/iVotronic/ballot style/race level, votes from the "vote cast" codes, and votes from the results file. Discrepancies between these files usually indicate that procedures have not been followed. I verify that iVotronics used for voting have been closed and that the PEB used for closing shows up in the system log file as having the correct number of votes uploaded. I verify that all the memory cards have been collected and their data uploaded, and I identify instances in which the ballot definitions in Unity differed from those in the iVotronics. I also record lists of the events in the event log that indicate that the machines have been malfunctioning and thus might not be recording votes correctly or might not have recorded the correct data, although I am not able to determine what the incorrect entries might be.

38. I have over the course of four General Elections now seen instances of probably all the different errors that could occur. Assuming there is a record in these files of any of the hardware by serial number, then my programs will detect an inconsistency and report that in an EXCEPTIONS file.

***Conclusion: A Forensic Audit Is the Only Way to Have Confidence in the Vote Tally***

29. For the reasons stated above, the electronic voting systems in place in Pennsylvania (including Allegheny County) are unreliable and vulnerable to attack. That is why other jurisdictions have discontinued the use of some electronic voting machines.

30. There were well-publicized attacks on America's voting infrastructure this year by foreign agents and other hostile forces, attacks confirmed by the United States' government's security agencies.

31. Given this reality, and given the vulnerability of the electronic machines used here, it is crucial that computer experts be able to forensically evaluate the electronic voting data from Allegheny county to ensure that the vote was counted accurately.

32. I affirm that the foregoing is true and correct.

Duncan Buell 2 Dec 2016

DUNCAN BUELL Date

Sworn before me this 2nd day of December, 2016, in Columbia, SC

Rebecca Mayo

NOTARY PUBLIC