SM

c/o 3548 Beechwood Boulevard
Pittsburgh, Pennsylvania 15217-2767
412-421-0178
voter@VoteAllegheny.org

VoteAllegheny Report on ES&S M650 Logic & Accuracy Testing Procedure

Report date June 3, 2007

Report author:

Collin Lynch

with David A. Eckhardt, Ph.D.

Clock loss is a problem for the iVotronics, so during this startup the clocks were set to the correct date and time for the present election.

At this time the iVotronic firmware was also 'checked' by county staffers. This check consisted of observing the software version number printed on the startup screen and noting any anomalies or deviations from 9.1.4.1. When asked, Elections representatives reported no such instances of errors.

(2) Automatic PEB test.

The automatic PEB test made use of a built in procedure of the iVotronic firmware. Said procedure utilizes a preprogrammed flash and PEB as well as an iVotronic. The flash card in question lists the sum total of possible candidates on the ballot. The PEB in turn is the Supervisor PEB for a given ward and district and has been preprogrammed with the ballot for that Ward and District. The Master PEBs were not employed as part of this process.

PEBs were grouped in boxes of 10. Roughly 14 banks of 10 machines each were available for use in this process. At the time I was present roughly five to six individuals were involved in the operation of iVotronic machines.

Each individual was given a box by one of the other staffers and proceeded to insert them into the machines. On each insertion they would start the system and select a procedure entitled "Multi-Vote L&A Test." This procedure would vote a simulated set of ballots for each location, casting one vote for the first candidate, two for the second, etc. The vote also produced a blank or undervoted ballot in each race. The exact process was unclear and various individuals described the ballots cast in different ways. Once the process began the individual would start the next PEB on the next iVotronic and so on. The entire simulation process ran in parallel.

This vote process also simulated the casting of write-in ballots but they were not retained or read off of the flash cards. It is unclear whether any text was even filled in. Once the ballot was cast the system was set to clear the terminal, thus removing, in theory any record of the ballots cast. No printed record was produced.

This process was said not to update the machine counters as it was a separate test procedure.

It took roughly 17 minutes for the process to be completed for each bank of ten.

Once the PEBs were completed, they were taken to a single laptop running Unity, where they were read in to have the total results checked. Anomalous total values or total votes for each Ward and District would have prompted a reexamination of the Ballot programming. The total number of ballots produced for the entire county was expected to be roughly 200 or more.

(3) Manual Ballot Style Test.

Following the initial test, the county commenced a manual ballot style test. The stated purpose of this test was to ensure that the ballots themselves were programmed correctly for style. Initially it had been proposed by ES&S staffers that this be an automated test with the ballot styles loaded and voted on by a system. This was overruled by County Staffers.

The decision was made to do an automated test of all 300-310 different ballot styles available in the county with each style covering one or more Wards and Districts apart from any split districts. As part of this process an absentee ballot for each style was collected along with a Supervisor PEB from each location.

Each pair was taken by a county staffer (roughly six were employed for this process) to a single iVotronic where the system was started up with the PEB and setup for the election. No zero tape was printed or verified. Each individual then went through two simulated Democratic votes, two simulated Republican votes, and one non-partisan vote. As the votes were cast, the staffer's hand marked the numbers on the printed (absentee) ballots that corresponded. This process was intended to be random with each individual selecting a slate of votes to cast as they wished seeing to it that each one tested some set of the ballot.

Once the ballots were cast the machine would be "closed" from election day procedures and a single result tape would be printed out. The resulting ballots would be accumulated on the Supervisor PEB. Once the printout was completed and the ballots cast the machine would be cleared using a "Clear and Test PEB" which required a password.

This entire process took roughly 15 to 20 minutes and seven county staffers were employed in it.

The resulting votes were intended to be tabulated using the same Unity laptop that was previously present. Said totals would then be compared on a Ward and District basis to the results listed on the printouts and the hand sheets. This was described largely as a storage test.

(4) Parallel PEB Test (Planned).

At the time of my observation a parallel activation test was planned for the PEBs. This process would use a bank of three iVotronics, each of which would be fed one of the three PEBs for a given Ward and District. Once inserted, the screen values would be checked to confirm that they brought up the same ballot and thus matched. Once all three were seen to have the "matching ballot" this test would be declared passed.

At the time of discussion this constituted the only L&A test that involved the Master PEBs.

At the time of my discussions it was unclear just how the equality of the three would be tested: *i.e.*, whether the designated Ward and District numbers would be matched alone or whether the three would be used to actually "bring up" ballots and then have those ballots visually inspected.

I did not observe this test and it is unclear when or if it took place or whether the terms of its performance changed.

(5) Activation Test of iVotronics.

Once all flash cards were completed, the county's plan was to then take a single Supervisor PEB or a special one-use PEB and to go to each of the 4,000+ iVotronics activating them to see if they brought up a ballot. This process would be conducted by a pair of individuals one of whom would insert a PEB and let the system get to the point where it would ask "Do you want to open the polls?" The second individual would select No and remove the PEB shutting down the system. Said process was slated to

merely involve this initial activation and each iVotronic would be declared acceptable as soon as it began to activate.

No other components were slated to be tested at this time. Once each machine passed. it would be closed up and sealed with a zip tie for delivery.

I did not witness this process and have not yet had the time to query county staffers regarding it.

(6) Audio Ballot Test.

Once the initial test process was completed. the plan was – time pending – to go to some as yet unspecified number of the audio-equipped iVotronics and to test the audio on them by walking through the audio ballot on a single PEB. I also did not witness this procedure and it is unclear how or if this was performed.

General Comments:

It is heartening to observe that the County's election procedure is more involved than in previous elections and that both an audio equipment test and manual ballot test were planned. County staffers should be commended for overriding initial ES&S suggestions in planning for the manual test.

It is disheartening to note that neither clock tricks nor a full-scale manual ballot test were performed. By leaving the clocks as-is. any election-day attacks from embedded code would not exhibit themselves save under extreme errors.

Ultimately. however. all of these procedures are focused on accidental. and innocent. ballot programming errors. None of them is designed for or capable of detecting a determined attack that involves the subversion or exploitation of elections software. Visual inspection of the printed serial numbers. automatic and manual ballot tests are inadequate. especially if said inspection is done on a day other than election day to detect any deliberately concealed attack.

As a simple point any portable code such as a virus could freely turn control of the system over to the original software on any day other than election day and thus escape detection.

It is worrisome by the fact that the L&A process involved no independent test of the Unity election systems which were assumed to be correct. Such assumptions based as they are on a faith in the minimal state or ITA inspections is misplaced. as revelations about security holes in other inspected systems has shown.

All of the pre-election analyses performed by the county make the assumption that this is a trusted environment where no determined attacker will seek to subvert an election. As the history of elections shows us. this is not the case. Historically elections have faced attacks from individuals and groups that are very real. very determined. and very well motivated. The very avenues left unchecked are those most likely to be exploited by a person with malicious intent. In order to protect ourselves. we must act with the assumption of a determined and well prepared attacker. a baseline assumption that is standard in the computer security community. Too much is on the line in elections for us to act otherwise.