Security and Reliability of Webb County's ES&S Voting System and the March '06 Primary Election

Dan S. Wallach
Associate Professor, Department of Computer Science, Rice University
May 2, 2006

(Data presented in this report was obtained, in part, by the attorneys of Campero & Becerra, and in part by myself and my graduate student, Dan Sandler, when we were allowed to directly observe and copy data from Webb County's voting systems, impounded as part of an ongoing investigation into the election results. My discussion includes some analysis prepared earlier by David Dill (a computer scientist at Stanford who, along with myself, studies the security issues with computers in voting systems). Dan Sandler and I wrote the software we used to analyze the election results.)

My expertise is in computer security, where I have been performing research since 1995. As a graduate student at Princeton, I helped find significant flaws in Sun's Java system, then being adopted widely in web browsers, that would allow a hostile web page to completely take over a web surfer's computer. Later, as a professor at Rice, I have also studied security issues that arise in a number of networked systems, including flaws we found in Google's Desktop Search (that would allow an outsider to see the results of local searches). I first considered electronic voting security issues after Harris County adopted Hart InterCivic's eSlate system in 2001. I was asked to testify before the Houston City Council about whether I felt this was a good idea. My opinion then, as now, is that paperless electronic voting systems introduce a wide variety of security issues to elections that appear not to have been given serious consideration by either the vendors or the state or federal certification standards. With HAVA (the Help America Vote Act of 2002) requiring "accessible" voting systems starting in 2006, and the grants it provides for voting system upgrades, electronic systems, such as have been deployed in Webb County, are being rapidly adopted, nationwide.

Before considering the details of the races in dispute, I will discuss the policies, procedures, and general security issues with Webb County's election systems. Webb County is somewhat unusual in giving voters the choice of voting on paper (using optical scan ballots that are centrally tabulated with an ES&S Model 650 scanner) or voting electronically (on ES&S iVotronic touchscreen systems). Webb County chose not to purchase any of ES&S's Model 100 precinct-based optical scanners.

Voters also had the option of early voting at a number of voting centers (any voter can visit any voting center and, after proper identification is presented, will be given the proper ballot for his or her home precinct) or election-day voting at their home precinct.

Threat Analysis

Any security analysis must begin by discussing the threats that a system might face, and how those threats are mitigated through the use of appropriate technologies, policies, or procedures. Inadequacies can generally be identified well before a system is deployed in the field. Hopefully they can be addressed beforehand as well. The following list is just the tip of the iceberg.

1) Software tampering in voting machines (pre-election)
    a. The ES&S iVotronic systems, as used in Webb County, appear to be special-purpose devices, suitable only for voting. Inside, however, they are built from the same parts as general-purpose personal computers and the software that drives them could potentially be reverse-engineered, modified, and reloaded into the machine. If this were to occur, there would be no evidence whatsoever. The iVotronic systems print their software version whenever they are turned on, but malicious software could always still print the proper version. Similar issues apply to the "protected" and "public" counters, the event logs, and the votes themselves.
    b. In order to install new firmware in an existing iVotronic (for good or for evil), the operator must go through the following steps:
        i. Hold down the "Vote" button while inserting a "supervisor PEB"
        ii. After a few seconds of the machine beeping, release the "Vote" button
        iii. Type in the "service" password
        iv. Select the "Election Central" menu
        v. Type in another password
        vi. Select the "Upload Firmware" option
    c. At this point, a firmware image is read from a CompactFlash memory card and stored inside the voting machine. Of note, there is no corresponding "download firmware" option that might otherwise be useful to audit that a machine was running "official" firmware, nor are there any other mechanisms to allow an auditor to assess whether the firmware within the machine matches any "official" version.
    d. The systems used in Webb County use the default passwords, as shipped from ES&S. These passwords are only three characters long and are presumably widely known[1]. ***Webb County must change its iVotronic passwords!*** Furthermore, ES&S should not ship systems with such easily guessed passwords. Physical security measures cannot be solely relied upon to dissuade a motivated and skilled attacker, nor can the obscurity of the firmware be assumed to deter its reverse engineering. An attacker

[1] The selection of poor passwords has been discussed by other examinations of the ES&S iVotronic, including the Pennsylvania's certification report, written by Dr. Michael Shamos in 2006, and Compuware's report, prepared for Ohio in 2003. The Compuware report states that the supervisor password is stored, unencrypted, in the CompactFlash audit data and that there are two hard-coded passwords. Hard-coded passwords are *never* acceptable.

must be presumed to have a legitimate copy of the iVotronic software from which to derive a corrupt version.

   e. As a result, the only meaningful security measure that presently prevents an attacker from installing malicious firmware is the need to possess a supervisor PEB. While a regular voter might not be able to accomplish this attack without being caught by an astute poll worker, a malicious poll worker would have all the necessary tools and would have the necessary opportunity to perform such an attack, as would any county employee who had access to the warehouse in which voting machines were stored between elections.
   f. Version 9 of ES&S' software allows for better passwords (six characters long, at least as used in Pittsburgh, PA) and segregates the firmware upgrade option behind its own password that need not be given out to poll workers. Version 8, the latest version currently certified in Texas, does not have this valuable security feature.

2) Voting machine tampering (during the election)
   a. During an election, a normal voter may attempt to tamper with an iVotronic system while in the voting booth, which offers some measure of privacy. As pointed out by Michael Shamos in his recommendations for Pennsylvania's use of ES&S's iVotronic systems, the CompactFlash slot, the serial port, and the power plug are directly accessible to the voter. Even an unsophisticated voter could simply unplug the machine, forcing it to consume its limited battery power. Likewise, a voter could simply steal the CompactFlash card; the iVotronic uses cards that are compatible with many digital cameras. Pulling out the card exposes the tiny, easily damaged pins that are used to connect to the card. Furthermore, the iVotronic does not allow for "hot plugging" of CompactFlash cards, even though current laptop computers and cameras do it just fine. Simply pulling out and replacing the card can cause an iVotronic to "stick", requiring the use of a paper clip to press a recessed "reset" button.
   b. A more sophisticated voter could attempt to perform the software tampering attack, as described above, although it would require the voter to have a suitably prepared PEB, perhaps hidden in a jacket pocket. The iVotronic's beeping might or might not be a sufficient deterrent, depending on whether the poll workers are trained that such beeping is cause for alarm. (In addition to uploading new firmware, those menus also contain an option to clear the machine of its votes. Again, stronger passwords are essential to the iVotronic's security. ES&S's Version 9 software partially addresses these concerns, but it is not presently certified for use in Texas.)

3) Ballot stuffing by poll workers
   a. A legitimate poll worker has all the necessary tools to cast additional votes. While some voting systems, such as the system being adopted in India, limit the speed with a voter can cast votes, no such rate limitations are built into the iVotronic. If the number of votes is greater than the number of voters who signed in, this would *hopefully* be detected after the

fact, as all the necessary information is present, but there would be no way to identify the fraudulent votes. The iVotronic's event logs indicate times, to the second, for when votes are cast, but the recorded ballots are apparently randomized, as a measure to increase voter privacy, and thus prevent voter bribery and coercion. **This randomization makes it impossible to identify and individually remove fraudulent votes.**

b. Traditionally, poll worker fraud is deterred by having mutually distrusting poll workers (e.g., pairing up Republicans with Democrats). Webb County's population appears to be skewed strongly toward one party, making it difficult to identify natural safeguards against such misbehavior.

c. Of course, ballot stuffing is an old threat. In this respect, electronic voting systems like the iVotronic represent a modest improvement over traditional paper ballots, because the event log may be able to identify misbehavior (later, I will describe some anomalies we found in the event logs).

4) Software tampering in the tabulation system

a. Systematic tampering with voting machines might leave enough traces to be detected, but centralized tampering with the election results might be much simpler. While I have not had the opportunity to inspect the ES&S "Unity" tabulation system, I understand that it is a standard application that would run on Windows 2000 or Windows XP. **As such, the tabulation system must never be connected to the Internet at any time.** ES&S offers the use of modems to deliver election results over the telephone. A modem offers as much access to the system as the Internet, and as such, modems should never be used. Only an "air gap" defense will have any hope of keeping the wild world of Windows security flaws from being easily exploited to corrupt the election outcome. Even then, physical access to the tabulation systems must be carefully limited, and proper Windows security measures, such as selecting good passwords, should be used. I have no information as to whether such proper procedures were performed in Webb County.

b. Similarly, the zero tapes and end-of-election tapes, printed in the polling place, can and should be audited against the official tallies as a matter of course for the election administrator. Such audits are critical to detecting if any tampering might have occurred in the election tabulation.

c. Likewise, the PEBs and CompactFlash cards can and should be used for regular audits, to double-check that the official tabulation was correct. Such audits should be performed by separate staffers using separate computers. If the official tallies are computed using PEBs, the audits should be performed using the CompactFlash cards. By separating the tally mechanisms from the audit mechanisms, fraud becomes far more difficult to perform without discovery.

d. Finally, the iVotronic system has three internal memory units where it stores copies of the election results. **These internal memory units must be audited as well**. Reading these memory units uses the same password-protected menus as described above. The memory contents are written to a CompactFlash card. While performing such an audit on every iVotronic may require non-trivial labor, certainly a percentage should be randomly selected for auditing, and those results should be compared to the official results. If an inconsistency appears, then further auditing would be required.

   e. When auditing determines contradictory results, a complete audit must be performed against the original iVotronic machines (to best eliminate the possibility of tampering with data in transit). As a result, all iVotronic machines must be impounded until all election contests have been resolved. Alternately, if the machines must be used before a contest is resolved, their internal memories must first be saved to separate CompactFlash cards before the iVotronics are cleared for the next election. Representatives for the candidates contesting the election results should have the opportunity to observe this process and to make their own (digital) copies of the data being extracted.

5) Data tampering in the tabulation system
   a. My own analysis is based, largely, on event logs and voting logs which were centrally generated and include all iVotronic systems used in the election. This data could well have been corrupted, either as a result of software tampering, as described above, or by the actions of a malicious insider. Such an insider could potentially insert a USB memory stick or a CD-ROM with hostile software that would directly manipulate the voting records stored by Unity. If the malicious software was properly written, it could inject votes, delete votes, or flip votes, and would leave no evidence of its having been used. The only solution to such a problem is to "lock down" the tabulation system. Windows XP supports such modes of operation, although they are widely regarded as painful to use, but this is precisely the sort of environment where these measures are appropriate.

6) Tampering with vote transmission
   a. ES&S iVotronic systems support a number of techniques for collecting the votes from a precinct and sending them to be tabulated. The mechanisms used in Webb County are PEBs and CompactFlash cards. PEBs are powered by internal batteries and speak to the iVotronic system using infrared LEDs (in the same fashion that TV remote controls speak to a TV set). By virtue of being an entirely proprietary system, no other vendors offer systems that will interoperate with PEBs. This provides a primitive level of protection against tampering. It also, unfortunately, makes PEBs difficult to audit without having additional ES&S equipment present. I have no reason to suspect that an attacker could not reverse-engineer a PEB and build a compatible replacement.
   b. CompactFlash cards are a widely used standard. We copied and examined the memory cards used to record the early voting in Webb County. Unfortunately, the election results are stored in a proprietary, binary file format, and we do not have suitable ES&S tabulation systems available to tabulate them in the official manner. Interestingly, there appears to be no cryptography of any kind protecting these files. The binary file format

structure will require us to do more work to decode it, but we see no inherent reason why it could not be done. As such, **the present CompactFlash cards do not provide adequate protection against tampering while in transit**. Any laptop computer would be able to tamper with the contents of one of these cards in seconds.

   c. Version 9 of ES&S's software apparently "encrypts" the contents of these CompactFlash cards[2]. If this is true, the only purpose it would serve would be to increase the difficulty for third parties to audit election results. Digital signatures, however, would be quite valuable to protect data from tampering in transit. For contrast, Hart InterCivic's eSlate "mobile ballot box" uses digital signatures (according to a Symantec report, commissioned by Hart InterCivic[3]).
   d. ES&S should not rely on an obscure, binary file format. Instead, ES&S should write out data that is easily read by other software (perhaps in an XML-style syntax), and they should gain security through the use of cryptographic digital signatures, among other widely used mechanisms. Such procedures would greatly aid the process of independent election audits, allowing third-parties to conduct their own recounts without requiring ES&S software.

7) Procedural mishaps: incorrectly tabulating "test" votes
   a. ES&S iVotronic systems have a "clear and test" function built-in. However, an election administrator who wishes to perform "Logic & Accuracy" tests must test the whole system, with fake voters casting their votes under controlled circumstances, such that the tabulation's results are known in advance. In the Webb primary election, we observed a number of votes cast on dates other than March 7 in iVotronic systems that were only supposed to be used on March 7. These machines had no votes whatsoever cast on March 7. Most of these machines had only two votes cast (typically one Republican and one Democratic), strongly suggesting that these were "test" machines, yet their votes appear in the official tallies.
   b. The tabulation software needs to have "sanity checks" built in that can detect such anomalies. Furthermore, the iVotronic systems should know the date of the election and refuse to accept votes outside of this date. Regardless, the election officials, themselves, should have discovered these anomalies long before publishing their results.

8) Dealing with "incomplete" votes
   a. A voter is entitled to "flee" before casting their ballot. Certainly, some of these voters thought they were done and didn't realize they had to press the "Vote" button first. In Webb County, the logs indicate a number of "Super ballot cancel" instances, where a poll worker followed the

[2] I was asked to testify as an expert witness in Taylor v. Cortés (U.S. District Court, Western District of Pennsylvania, Civil Action No. 06-481) concerning the security of ES&S systems. The defendant's attorney described this new "encryption" feature in version 9 of the ES&S iVotronic software, asking me what impact it would have on my findings.

[3] `http://www.sos.state.tx.us/elections/forms/sysexam/hart_symantec_security.pdf`

procedure to discard these ballots. It's possible that these voters experienced machine problems and were directed to use other machines. It's also possible that they thought they had selected their candidates and misunderstood how to operate the system. **Webb County must institute procedures to carefully track the circumstances surrounding any use of "supervisor" privileges**, including canceling a ballot. For every one of these instances, there should be a written record to explain exactly what happened and why. Webb County already has elaborate procedures for witnesses who must observe and sign a log whenever seals are broken on a container with voting records. Similar procedures must be used in these circumstances.

9) Using thermal printers / thermal paper in a hot climate
   a. The printer used by Webb County uses thermal paper. Similar printers and paper are often used to print restaurant or gasoline receipts. Heat causes thermal paper to turn black. In a climate as warm as South Texas, thermal paper seems like a poor choice for important election records. On the other hand, thermal printers have no ink cartridges or ribbons to replace, making them very reliable. Unless a better printer can be found, **storage and transportation of the printed paper tapes must be temperature and light controlled**.

10) Registration / calibration issues with the touch screen
   a. We hear the same anecdotal stores any time a touch-screen voting system is deployed. "I touched the button for *A* and it lit up the button for *B*." The most common cause of this problem is one of *calibration*. Every PalmPilot user has observed the same effect. The place you click is not exactly the place it thinks you clicked, but you can go to the calibration screen, it shows you cross-hairs, and you click in the center of each. You get it just right, but if you use it again at a different angle, the calibration doesn't work right again. It changes depending on the viewing angle. This same issue applies to every touch-screen voting machine.
   b. When I was operating several of Webb's iVotronic systems, I found I had to aim for the button *below* the one I wanted to press. It was a very frustrating process, and I'm certain that many voters experienced it as well. ES&S could partly improve this by using much larger on-screen buttons (also benefiting voters with reduced visual acuity).

11) Vendor dependence
   a. The ES&S iVotronic operations manual has a long list of possible malfunctions and how they should be resolved. The overwhelming majority of these issues say "Call ES&S". The vendor should not need to be involved, even when things go wrong[4]. The voting system should be designed in such a simple and straightforward manner that it would be easy for a third-party to diagnose and repair problems. This would

[4] Dana DeBeauvoir, the county clerk of Travis County, has often said that when Travis County procured its Hart InterCivic voting system, the vendor was invited in to teach them how to use the system and was then asked to leave. If Travis County can operate its election systems without needing help from its vendor, Webb County should insist on a similar level of vendor independence.

improve transparency in the election process, giving candidates greater ability to see “under the hood” and convince themselves that the election results are accurate. Furthermore, in the event that these voting machines outlast their vendor, third parties would be able to figure them out and service them.

Many of these tampering issues are the result of the malleability of computer storage and computer software. A computer will blindly follow whatever instructions it is given. If there are flaws in those instructions, or if the instructions can be replaced, then anything becomes possible. Likewise, digital storage can be easily written and easily overwritten. While a number of cryptographic techniques ostensibly *can* be used to prevent tampering with the computer storage while it is in transit, we cannot easily verify, from outside, whether the machine software is operating correctly. This ultimately boils down to a lack of *transparency* in the election system. Neither an election observer, during the election, nor an after-the-fact auditor has much if any evidence to convince them that they can see everything going on under the hood. While some obvious problems might manifest themselves (e.g., more votes cast than voters signed in), others might never be detected.

For this specific reason, a large number of computer science researchers and others have favored the use of paper ballots in conjunction with electronic voting systems. Such hybrid systems (sometimes called voter-verifiable paper audit trails or VVPAT) preserve many of the benefits of paper (notably its permanence and relative immutability) while also having the benefits of computer systems (event logs, accessibility features, etc.).

Election Results Analysis

In the limited time available, we chose to focus our analysis on the “event logs” and “image logs” which we were provided to us by Campero & Becerra. Event logs look something like this:

```
WEBB COUNTY, TEXAS
                                   PRIMARY ELECTION
                                   MARCH 7, 2006 RE-COUNT LOG
RUN DATE:03/24/06 02:14 PM
ELECTION ID: 6PTXWEBB

Votronic  PEB#   Type    Date       Time     Event

5117865  161061  SUP   03/06/2006 16:31:12   01 Terminal clear and test
         161126  SUP   03/07/2006 07:09:37   09 Terminal open
                       03/07/2006 07:13:50   13 Print zero tape
                       03/07/2006 07:15:39   13 Print zero tape
         160973  SUP   03/07/2006 12:32:24   20 Normal ballot cast
                       03/07/2006 16:59:19   20 Normal ballot cast
                       03/07/2006 18:06:23   20 Normal ballot cast
                       03/07/2006 18:25:56   20 Normal ballot cast
                       03/07/2006 18:32:18   20 Normal ballot cast
                       03/07/2006 18:48:54   20 Normal ballot cast
                       03/07/2006 18:56:03   20 Normal ballot cast
                       03/07/2006 19:01:52   20 Normal ballot cast
         161126  SUP   03/07/2006 19:39:41   10 Terminal close

5140052  161061  SUP   03/07/2006 15:29:03   01 Terminal clear and test
         160980  SUP   03/07/2006 15:31:15   09 Terminal open
                       03/07/2006 15:34:47   13 Print zero tape
                       03/07/2006 15:36:36   13 Print zero tape
         160999  SUP   03/07/2006 15:56:50   20 Normal ballot cast
                       03/07/2006 16:47:12   20 Normal ballot cast
                       03/07/2006 18:07:29   20 Normal ballot cast
                       03/07/2006 18:17:03   20 Normal ballot cast
                       03/07/2006 18:37:24   22 Super ballot cancel
                       03/07/2006 18:41:18   20 Normal ballot cast
                       03/07/2006 18:46:23   20 Normal ballot cast
         160980  SUP   03/07/2006 19:07:14   10 Terminal close
```

These are records for two different iVotronic systems that were used on March 7. The first machine was cleared and tested the day before Election Day, as were the majority of the iVotronic systems used in the election. The second machine was cleared at 3:30pm on Election Day and used until 7:07pm. Any votes or records from earlier in the day are completely lost, because the “clear and test” operation clears everything. This machine also had a cancelled ballot, perhaps the result of a voter “fleeing” before pressing the “Vote” button.

So, maybe something fishy was going on in the precinct with machine #5140052. It appears to have been the sole iVotronic machine in use in precinct 225. Were there additional votes cast but lost due to poll worker problems? The event logs don’t say any more, but we later studied the zero and results tapes, printed from this iVotronic. The “protected counter” indicated that twelve votes had been cast in the lifetime of the machine. Subtracting the six votes shown above, we can conclude that **a maximum of six votes may have been lost** as a result of this machine having been cleared. We do not have sufficient information to determine if these six votes were cast and lost on Election Day or whether they were cast earlier on the machine, perhaps as part of its acceptance testing.

Overall, we found twelve different machines that were cleared on Election Day. In addition to the above machine, we found machine #5146712, which claims it was cleared on 3/07 and had votes on 3/08. Most likely, the clock was off by a day, as with machine #5142523, described below. The remaining ten machines were both cleared and used on Election Day, with the time of the “clear and test” event occurring between 8 and 10am. If voters arrived before this and used one of these machines, their votes would have been irretrievably destroyed. The poll worker’s manual does not describe any circumstance under which a poll worker should use the “clear and test” option, and all of the other machines were cleared in advance. Further analysis would require studying the voter sign-in logs, to see if more voters arrived than votes were cast in these particular precincts. Likewise, we could examine the protected counters, as we did with machine #5140052, to determine an upper bound on the number of votes that may have been lost.

Here’s another suspicious machine:

```
Votronic  PEB#   Type    Date       Time      Event
5142523  161061  SUP   02/26/2006 19:07:05   01 Terminal clear and test
         161115  SUP   03/06/2006 06:57:23   09 Terminal open
                       03/06/2006 07:01:47   13 Print zero tape
                       03/06/2006 07:03:41   13 Print zero tape
         161109  SUP   03/06/2006 10:08:26   20 Normal ballot cast
                       03/06/2006 12:39:05   20 Normal ballot cast
                       03/06/2006 14:49:33   20 Normal ballot cast
                       03/06/2006 15:59:22   20 Normal ballot cast
                       03/06/2006 18:01:45   20 Normal ballot cast
                       03/06/2006 18:10:24   20 Normal ballot cast
                       03/06/2006 18:26:52   20 Normal ballot cast
                       03/06/2006 18:29:18   20 Normal ballot cast
                       03/06/2006 18:39:41   20 Normal ballot cast
                       03/06/2006 18:44:24   20 Normal ballot cast
         161115  SUP   03/06/2006 19:29:00   27 Override
                 SUP   03/06/2006 19:29:00   10 Terminal close
```

Was the clock simply off by a day, or was this machine used (illegally) on the day before the election? All of the votes cast on that machine were in the Democratic primary. Five of the votes were for Manuel Flores and three were for Joe Lopez. Precinct 416 had this machine as well as two others. Both had votes exclusively on March 7 (as they should), one with 17 votes and the other with 29 votes. Perhaps the "March 6" votes are legitimate but the dates are wrong. On the other hand, consider this machine:

```
Votronic  PEB#   Type    Date       Time      Event
5145172  161061  SUP   03/06/2006 15:04:09   01 Terminal clear and test
         161126  SUP   03/06/2006 15:19:34   09 Terminal open
         160973  SUP   03/06/2006 15:26:59   20 Normal ballot cast
                       03/06/2006 15:30:39   20 Normal ballot cast
         161126  SUP   03/06/2006 15:38:37   27 Override
                       03/06/2006 15:38:37   10 Terminal close
```

The vote image log for this machine has two votes, one cast in the Democratic primary and the other in the Republican primary (the Democratic primary vote favored Joe Lopez). The precinct in question (#133) had four other iVotronic machines. Three of those have what appear to be normal votes. The other (machine # 5147194), also has two votes on March 6 – one Republican and one Democratic (with the Democratic vote also favoring Joe Lopez). Overall, our analysis found 93 "Election Day" votes cast on 30 machines on days other than Election Day. Four of the machines might have simply had incorrect dates (with 5, 8, 10, and 17 votes recorded), while one machine had three votes and the remaining 25 machines had precisely two votes, each. If we tally all 93 non-election-day votes, Joe Lopez received 49 votes and Manuel Flores received 14. If we only consider the 26 machines with only two or three votes apiece, then zero votes appear for Manuel Flores, with all 27 votes appearing for Joe Lopez.

The most likely explanation is that these 26 machines were "tested" but their test votes were accidentally used in the real tally. Errors like this should have been caught in advance and could be caught better in the future if the test machines and their corresponding PEBs and Compact Flash cards were clearly and visibly labeled (e.g., with neon-colored tape) to avoid any confusion between "test" and "production" machines.

We also looked for evidence in the logs of other problems, including rapid voting (a possible indicator of ballot stuffing) or after-hours voting. Aside from the issues described above, we found nothing suspicious.

Subsequently, we went to verify that the dates on the voting machines described above were or were not correct. In searching through the impounded machines, we were able to locate 20 out of the 30 machines, list above, that we wished to inspect for possibly faulty dates[5]. In all cases, machines that appeared to have incorrect dates in the tallies did, in fact, have incorrect dates when we subsequently inspected them. Machines that we suspect had test votes appeared to have the proper dates set. This further supports the conclusion that four machines were used which had erroneous dates, with no poll worker

[5] The other ten machines were most likely present in the impound, but due to their dense storage and easily detached precinct labels, it was a difficult, laborious process to locate any particular voting machine. As a result, we were satisfied that locating and examining 20 of the desired 30 machines would be sufficient.

or election official taking any steps to correct this issue, while 26 machines were tested the day prior to Election Day, with their test votes being erroneously included in the official election tallies.