Voting System Examination
Election Systems & Software (ES&S)

Prepared for the
Secretary of State of Texas

James Sneeringer, Ph.D.
Designee of the Attorney General

This report conveys the findings of the Attorney General's designee from an examination of the equipment listed, pursuant to Title 9, Chapter 122 of the Texas Election Code, section 122.036(b).

Examination Date	January 18-19, 2007
Report Date	February 20, 2007

ES&S offers a complete line of products for every aspect of conducting an election, including election setup, DRE, optical scanning, tallying, reporting and auditing.

Components Examined	**Version**	**NAESED Number**
Unity Election System Software, which includes the following components	3.0.1.1	N-2-02-22-22-007 (2002)
- Election Data Manager (EDM)	7.4.4.0	N-2-02-22-22-007 (2002)
- ESS Image Manager (ESSIM) including Ballot on Demand (BOD)	7.4.2.0	N-2-02-22-22-007 (2002)
- Hardware Program Manager (HPM)	5.2.4.0	N-2-02-22-22-007 (2002)
- Data Acquisition Manager (DAM)	6.0.0.0	N-2-02-22-22-007 (2002)
- Election Reporting Manger (ERM)	7.1.2.1	N-2-02-22-22-007 (2002)
- Audit Manager	7.3.0.0	N-2-02-22-22-007 (2002)
- iVotronic Image Manager (iVIM)	2.0.1.0	N-2-02-22-22-007 (2002)
iVotronic DRE, 12” Non-ADA with Real-time Audit Log (RTAL, a VVPAT)	9.1.6.2	N-2-02-22-22-007 (2002)
iVotronic DRE, 12” ADA with 3-button audio and Real-time Audit Log (RTAL, a VVPAT)	9.1.6.2	N-2-02-22-22-007 (2002)
iVotronic DRE, 12” Supervisor Terminal	9.1.6.2	N-2-02-22-22-007 (2002)
iVotronic DRE, 15” Supervisor Terminal	9.1.6.2	N-2-02-22-22-007 (2002)
iVotronic DRE, 15” Non-ADA with Real-time Audit Log (RTAL, a VVPAT)	9.1.6.2	N-2-02-22-22-007 (2002)
iVotronic DRE, 15” ADA with 3-button audio and Real-time Audit Log (RTAL, a VVPAT)	9.1.6.2	N-2-02-22-22-007 (2002)
iVotronic DRE, 15” ADA with 4-button audio and Real-time Audit Log (RTAL, a VVPAT)	9.1.6.2	N-2-02-22-22-007 (2002)
Communication Pack with Printer	(None)	N-2-02-22-22-007 (2002)

Seiko Printer	(None)	(None)
Compact Flash Multi-Card Reader/Writer (Gang Burner)	9.1.0.0	N-2-02-22-22-007 (2002)
M100 OMR Precinct Ballot Counter	5.2.1.0	N-2-02-22-22-007 (2002)
Metal Ballot Box for Precinct Counter	(None)	(None)
M650 Central Count Tabulator (v. 1.0, red light)	2.1.0.0	N-2-02-22-22-007 (2002)
M650 Central Count Tabulator (v. 1.1, green light)	2.1.0.0	N-2-02-22-22-007 (2002)
AutoMARK Voter Assist Terminal	1.1.2258	N-2-02-22-22-007 (2002)
AutoMARK Information Management System	1.2.18	N-2-02-22-22-007 (2002)

Ballot Marking: Characteristics of the AutoMark Voter Assist System

Voting	Marks paper ballots based on choices entered on a touch screen by the voter. Prevents overvotes and warns of undervotes, just like a DRE.
Election Setup	Reads the election setup created by Unity. Can also be manually programmed to work with ballots of other vendors.
Tabulating	None. The resulting paper ballots are tabulated by other means, such as a scanner.

Voting: Characteristics of the Votronic and iVotronic DRE

Election Setup	Personalized Electronic Ballots (PEB) and separate flash memory cards are created with Unity software. Nothing is pre-programmed in the terminals; all the election information is in the PEB and flash memory. Anything that is precinct-specific goes in the PEB. The flash memory is only required if the election is large or there are image or audio files.
Zero-total report	On the thermal printer in the communication pack.
Authorization to vote / Ballot selection	There are two modes: • At the voting station, the voter inserts a PEB, which was initialized at a Supervisor station using a supervisor PEB. (The supervisor PEB and station are both red in color, to distinguish them from voting stations and voter PEB's.) The voter's PEB cannot be reused without re-activation. • Poll worker inserts a supervisor PEB into a voting station, immediately removes it, and selects the appropriate ballot. The supervisor PEB is retained by the poll worker and is reusable without re-activation.
View / Vote	LCD display / touch screen
Vote Storage	Three redundant flash memories
Precinct Consolidation	Allowed using PEB's. An audit log of this is kept in memory and can be printed at the precinct.
Transfer Results	PEB transported or data transmitted by modem to Unity software (or a regional site from which data is sent to the Unity software at central counting). The data is protected by a Cyclical Redundancy Check (CRC).
Print precinct results	On the thermal printer in the communication pack.
Straight party / crossover	Yes. A straight-party vote cannot cancel crossover votes that have already been selected, which protects the voter against mistakenly canceling a crossover vote.

ADA	Yes, but ADA capability is verified separately by the Secretary of State's office, so it was not demonstrated to the examiners. Because it is battery-powered, the iVotronic can be taken to the curbside for voting.
Voter-Verified Paper Audit Trail (VVPAT)	There is an optional VVPAT, called a real-time audit log, or RTAL. For privacy, the RTAL is maintained on a spool of paper that is enclosed in the voting station and viewed through a glass window. When a voter finishes, the paper is automatically advanced so the next voter cannot see it. Votes cannot be cast when the RTAL is not working. See below for details of the VVPAT.

Setup & Tabulation: Characteristics of the Unity System

Tamper Resistance	Cyclical Redundancy Check (CRC) on each record in the election files.
OS access	Not permitted during tabulation.
Real-Time Audit Log	Yes. This is a real-time printer that logs events at the central counting station. It should not be confused with the DRE's voter-verified paper audit trail (VVPAT) which ES&S calls a real-time audit log, or RTAL.
Data Integrity	There are no special transaction-processing features. According to ES&S, there is no need for such features because all the data is written in a single write statement, making it impossible for partial results to be entered into the database. Also, it is easy to recalculate everything if a problem is suspected, and everything is automatically re-calculated when you request a canvass report. Since a canvass report would always be requested, this is satisfactory. In short, it is nearly impossible to get an incorrect result and not know it.
Notes	• The Data Acquisition Manager is used in regional centers to collect precinct data for forwarding to central counting by modem or by carrying a PEB. • The Data Acquisition Manager does not need to know election-specific data or understand the results. It does not tabulate, but merely stores packets and then forwards them.

Examination Procedures

This was a two-day examination, and there were two changes in procedures from previous exams:

- On the first day of the exam, Steven Berger and I verified that the vendor's installation CDs matched official CDs that were obtained directly from Systest. This was done by booting from a CD containing a hashing program and comparing hash codes from the Systest CDs with hash codes from the vendor's CDs. We used this procedure because hash codes were not available from the NIST Voting Software Reference Data website (www.nsrl.nist.gov/votedata.htm).

  After verifying the vendor's CDs, we used them to install the software, thereby verifying that we were testing the same version that Systest approved. There was one problem, which is noted below under **Concerns**, but I am satisfied that we tested the correct version.

While this process was very educational, it is also very time consuming and of questionable value. I can see little motive for a vendor to bring a different version, so I'm not sure we need to do this in the future. There is a potential motive for an attacker to use a different version in an actual election, so it would be good to verify that the version actually used in elections is the same as the one certified. However the procedure we used would be extremely time-consuming and requires high skill, making it prohibitively expensive to perform in every jurisdiction. Perhaps a better way can be found.

- We agreed in advance to divide up the various tasks among the examiners. This allowed us to go into greater depth on each component, but it also meant that most results were not personally observed by every examiner.

  I personally observed the verification of the software's hash codes and the testing of the 15-inch iVotronic DRE with the real-time audit log, or VVPAT. For the other results, I depended on information from the other examiners.

Comments

- ES&S did not seek recertification of the model 150 and 550 scanners. The Optech Image Manager is also being phased out. Therefore these products can no longer be used in Texas. ES&S reports that there are fewer than 20 affected Texas customers, and that they are offering a liberal trade-in allowance so those customers can get a model 650 scanner. Some small customers may want to use a model 100. See below under **Concerns** about using the model 100 as a central-count scanner.
- The iVotronic DREs now support provisional ballots.
- ES&S has added a "soft" button on the touch screen for "Cast Ballot" in addition to the permanent, red "Cast Ballot" button. This is a nice addition, because it makes it easier for the voter to find the "Cast Ballot" button.
- A particularly clear message appears when an overvote is attempted, making it easy to recover.

VVPAT

Unlike some VVPATs, the ES&S Real-Time Audit Log (RTAL) does not permit the entire ballot to be reviewed at once. Instead, the RTAL lives up to its name by immediately recording each action the voter takes. If the voter does not vote in ballot order, the RTAL will also be out of order. If the voter makes a change, the RTAL will record the original selection and later the new selection.

This approach makes the RTAL easier for the software engineers to implement, but not necessarily for voters to use. First, there is no need for the programmer to deal with the problem of a voter's rejecting the ballot on review, because the voter can simply make a new selection, which appears at the end of the RTAL, signifying that it replaces the old one. The last selection printed is the only one that counts for that race. Second, the programming problem of displaying

a ballot that is longer than the window is solved; the voter must view the log entries during actual voting, before they scroll out of the window.

From the point of the voter or someone doing a manual recount, it is more difficult to tell from the log exactly how the ballot was voted, because the entries are not necessarily in order and obsolete selections may appear in the log, which is potentially confusing. Also, the voter must remember to review each log entry while it is still in the window.

This type of VVPAT is probably acceptable, but I would like to see the results of some field testing. Obviously I cannot address whether it meets requirements or not, since there are no VVPAT standards in Texas.

Finally, since the VVPAT records the ballots in order, privacy can be compromised when the VVPAT paper spool is changed or if someone at the polling place keeps a record of the order in which people vote on a particular machine and later looks at the VVPAT.

Comments on VVPATs

The concept of a VVPAT is very attractive. As a technologist, I am very aware of the dangers of placing too much trust in technology. As a citizen, I am very aware of the need for an audit trail that every citizen can understand and have confidence in.

Nevertheless, it is premature to require VVPATs. The cost is very high and several problems are mentioned below under **Concerns**. An additional problem is the unreliability of printers, further increasing the cost and complexity of elections. Rushing to deploy VVPATs throughout the state will likely cause more problems than it solves, many of which we cannot anticipate. However, I do recommend that some jurisdictions be permitted to try VVPATs, so we can gain experience with them.

Follow-up from Previous Exams

- ES&S has changed the ERM to prohibit counting results of the same precinct twice, which was called ADD mode. The ERM now always operates in REPLACE mode. This is an improvement.

Concerns

1. **Problem Opening Election.** When we tried to test the DREs, none of them could initially be opened to begin voting. In particular, I personally observed that the 15" iVotronic with VVPAT could not be opened. Furthermore, I did not see any error message – just a number. (A communication from ES&S asserts that the message "Improper Database Version" was given. It is possible that this is the interpretation of the number I saw or that this message was displayed and I did not see it.) The problem was eventually solved by re-burning the PEBs and flash cards for the election. ES&S gave several possible reasons why this may have occurred, but whatever the technical details, it seems clear that the problem was caused by the reinstallation of the software on

the first day of the exam. Normally the election would be created first, the PEBs and flash cards would be burned next, and then the election would be conducted without reinstalling the software. Therefore, the situation we encountered was not typical.
Recommendation: Because this situation is very unlikely to occur in actual use, I do not recommend withholding certification. However, it does illustrate the fact that, from the perspective of an election administrator, this system is fragile, complex and inscrutable. ES&S has been in business a long time and must therefore support a variety of old equipment (even though they have retired some) and old code that has seen many changes. Finally, much has been learned about providing a good user experience in the time ES&S has been in business. These factors make it difficult for ES&S to produce an election system that can be easily operated by poll workers and election administrators, so I sympathize with their plight. Nevertheless, I believe ES&S should employ a user-centered design process to bring their system up to modern standards of usability and reliability. The system should be more robust, clearer, and easier to understand by untrained election workers. It would also be good if Texas were to require higher standards in this area, but that is very difficult because these characteristics do not lend themselves to the kind of objective measurements preferred by government regulators.

2. **Incorrect Ballot Count on ERM.** When the results were tabulated on the ERM central count system, the initial report showed only three ballots, which was incorrect because ten ballots had been voted. (Note: I did not personally observe this.) As I understand the explanation from ES&S, this happened because some audit data from a previous election was accidentally placed in the wrong directory and some test data in that directory caused the system not to issue the normal error message. ES&S pointed out that this audit data should not have been placed in that directory and that their procedures call for all such data to be cleared. Therefore this would not happen if customers followed their procedures. I accept their explanation. Furthermore such a mistake would never go undetected. However, this illustrates even more vividly the comments I made in the recommendations in item 1 under **Concerns**. How can we expect election administrators to solve such problems when ES&S employees, who are presumably much better trained and more experienced, have trouble solving them. Furthermore, (a) the system did not make it easy to detect and recover from the problem, (b) the explanation of what happened is highly technical and complex, and (c) it took ES&S' experts some time to diagnose and correct it. As much as possible, the events that occur should be explained to the user in terms that make sense to him, rather than in technical language that makes sense only to the programmer. This illustrates the need for the voting system to automatically perform steps and automatically detect errors whenever possible.
   Recommendation: Certification should not be withheld because of this problem, but ES&S should be required to correct it in reasonable period of time. Again, this underscores my points about the need to live up to the state of the art by creating robust, understandable, easy-to-use systems.
3. **Cannot Mix M100 results with iVotronic.** When tallying, you must tally the iVotronic results separate from the M100 results. If you try to tally one while processing the other, the system will reject it.
   Recommendation: I do not recommend withholding certification, but this further illustrates my recommendations in item 1 under **Concerns.**

4. **Automatic Zeroing.** It was suggested again during this exam that ES&S devices should automatically clear totals at the beginning of an election, but (obviously) not between sessions of early voting.
   Recommendation: I recommend automatic clearing whenever the system can reliably determine that it is needed. Certification should not be withheld because of this problem, but ES&S should correct it in a reasonable period of time.
5. **Discrepancies in Totals.** There were initial discrepancies in the totals that were reported by several components of the ES&S system, including the totals in the precinct report generated by the 15" iVotronic with VVPAT, which I personally observed. The VVPATs were very helpful in resolving these difficulties. In the end, all of the discrepancies were found to be due to errors by the examiners or in the manual tallies that we were comparing to. *None of the problems were due to the ES&S system, except as described above in item 2 under* ***Concerns***. Unfortunately, I did not personally see these problems resolved (not even for the DRE that I was observing), so I am relying on information from other examiners and employees of the Secretary of State.
   Conclusion: I have confidence that the all components of the system tally correctly, but I have not *personally* verified it.
6. **Double Selection.** It is fairly easy to select the wrong candidate on the iVotronic touch screen, or even to unintentionally select two candidates in a race where you can vote for more than one. ES&S should consider creating a dead zone between candidate names and making changes to prevent two selections from being made simultaneously.
   Recommendation: Although this is significant, it is not as bad as it may seem at first, because the voter does have visual feedback, which provides an opportunity to correct the error. Certification should not be withheld because of this problem, but ES&S should be required to correct it in a reasonable period of time.
7. **M100 for Central Count.** Since the M150 and M550 scanners can no longer be used in Texas, counties that have them will need new scanners. Most will get M650s, but very small counties may prefer the M100 for cost reasons. Unfortunately, the M100 cannot be used as a central count scanner in Texas, because it does not have a real-time audit log. (In this paragraph, the phrase *real-time audit log* refers to the Texas administrative requirement that all central count devices have a printer that logs all significant events as soon as they occur, and not to the ES&S feature with the same name, which denotes what is commonly called a *voter-verified paper audit trail*, or VVPAT.)
   Recommendation: In small counties, the need for a real-time audit log is less, and cost is a more important factor. Therefore, I recommend that the Secretary of State remove the requirement for a real-time audit log from counties with very small populations.
8. **Provisional Voting on DREs.** This feature was tested successfully, but it does depend on the manual assignment of unique numbers to each provisional ballot.
   Recommendation 1: Jurisdictions should be required to have procedures in place to make sure that the numbers are unique and correctly recorded. I recommend using a preprinted sheet of labels with unique numbers on them. For each provisional ballot, the number should be entered into the DRE and the sticker should be removed and placed on the documentation for the provisional ballot. This should minimize clerical errors.
   Recommendation 2: There is also a chance that an error will be made entering the number into the DRE. It would be best if ES&S would provide software to generate the unique numbers with two or three extra digits containing a hash of the other digits. Then

the DRE should check the hash to ensure that the number was entered properly. This would both guarantee unique numbers and detect virtually all entry errors at the polls. However, while this is a best practice, it should not be required for certification given the relatively small number of provisional ballots.

9. **Comparison of installation CDs with Systest CDs.** When we compared the ES&S installation CDs with the Systest CDs containing the tested versions, the hash codes showed that all the files were identical. However, 12 files had different names, although they were identical in content. The files were all audio files (.WAV) in the AIMS module, and in every case the filename on the Systest CD had been shortened. Apparently the files were accidentally written on a medium that does not support long filenames, and consequently were shortened to conform to what is commonly called the 8.3 format. In all likelihood the error was made by Systest while producing the CDs.
   Conclusion: I am satisfied that we tested the same version that Systest approved, since the content of the files was identical, and only the names were different. Therefore this is not an issue.
10. **Access to ERM through the DAM.** Although the Election Reporting Manager (ERM) computer is locked down during tabulation, as required in Texas, it is possible to access the ERM computer using the Data Acquisition Manager (DAM) computer, if they are on the same network. When using a network, the DAM places its result files into a folder that can be accessed by both computers, and the ERM finds the files there and processes them. ES&S says that they configure Windows security so that the DAM does not have access to any critical files on the ERM computer. The folder used for the transfer could even be on the DAM computer, in which case the DAM computer need not have access to *any* files on the ERM computer. However, this solution is not satisfactory, because Windows security could be reconfigured by a single person with the proper access. This event would not be logged because it takes place in Windows, not the ERM. If the configuration were later changed back, there would be no record, and the files on the ERM computer could possibly be tampered with during tabulation.
    Recommendation: The only solution I can see is to prohibit the ERM computer and the DAM computer from being connected to each other. Instead, the data would be moved by transferring a flash card from the DAM computer to the ERM computer. I hate to make a recommendation that causes extra work for election workers, but I see no secure alternative. Also, the data need not be transferred often. In theory, it only needs to be done once after the data for all the precincts are on the DAM computer.
11. **Undervote message on the poll-closing precinct report.** The iVotronics report an undervote on the poll-closing report for every voter who did not make a straight-party selection. From the perspective of a software engineer, I can see how this makes sense, but it is potentially confusing to poll workers, who think of an undervote as a deficiency, and might be concerned about the large number of undervotes. Also, when there are no undervotes, the "Undervote" heading is still printed on the report with no corresponding number, not even a zero. This is also a bit confusing. The word *undervote* by itself looks like it is reporting an undervote, when in fact it is intended to communicate that there were no undervotes.
    Recommendation: While these are not good design, they are not important enough to justify withholding certification.

12. **Using AutoMARK and the AutoMARK Information Management System (AIMS) with Scanners from other Vendors.** ES&S states that AutoMARK and AIMS can be used with scanners from other vendors and even read election setup from other vendors' systems. However, ES&S did not demonstrate this capability.
    Recommendation: AutoMARK and AIMS should not be certified for use with systems from other vendors until it has been adequately tested.
13. **VVPAT in English.** The VVPAT (called RTAL) is always printed in English, regardless of the language displayed on the DRE screen. I personally observed this on the 15" iVotronic with RTAL. We voted a ballot in Spanish, but the RTAL was in English. Although the RTAL consists mostly of candidate names, which should not be translated, voters who don't speak English should see the entire RTAL, including the office sought, in their language.
    Recommendation: The RTAL should be in the language being used, and the RTAL should not be certified until this is fixed.
14. **Changed Selections may be Confusing on the VVPAT.** When a candidate selection is changed, the old selection has already been printed, and remains visible on the paper. The new selection is printed at the end of the paper spool, which indicates a selection that supersedes the old one, but I fear that voters may find this confusing. It may also be confusing during a manual recount, but this is less of a problem because the people doing a recount will quickly gain the experience that allows them to understand what is going on. Nevertheless, it may increase the error rate during a manual recount. Of course this is not a problem for a recount done with a scanner. It only applies when a person is reading the printed log, either to verify that the bar code is correct or to make a manual count.
    Recommendation: This type of VVPAT should be tested to see if voters find it confusing. If it is a problem, ES&S should change to print only the voter's final selections.
15. **Must Check the VVPAT as you Vote.** Voters may not realize that they must check the VVPAT as they vote. If they do not, their first selections may scroll out of the window before they have been verified. This problem is exacerbated by the extra space left between selections on the VVPAT, increasing the likelihood that earlier selections will disappear.
    Recommendation: This type of VVPAT should be tested to see if voters find it confusing.
16. **VVPAT Privacy Issues.** Privacy may be compromised when the paper spool is changed or if someone at the polling place keeps a record of the order in which people vote on a particular machine, since the VVPAT records the ballots in order. We have previously required that voting machines not keep a list of ballots in the order they were voted.
    Recommendation: Privacy is a fundamental requirement. No VVPAT that records ballots in order should be certified until this issue is resolved. In particular,
    a) We should address whether procedures can prevent the compromise of privacy when the paper is changed, and if so, specify those procedures.
    b) It must be made clear in the law that a VVPAT is not an open record, and
    c) We should address procedures for maintaining the privacy of VVPAT records after the election.

Summary

The ES&S system is one of the best election systems available. I believe it is in the best interests of Texas voters to certify it, with the conditions and exceptions noted above.

The question has been raised whether each examiner must personally see every aspect of the system and inspect every result. As a technical examiner, I will leave that question to the lawyers, but I have indicated in this report what I personally saw.